IJCSIS Vol. 11 No. 7, July 2013
ISSN 1947-5500

International Journal of Computer Science & Information Security


Cornell University
Library


Cogprints


Google scholar


.docstoc
find and share professional documents


ScientificCommons

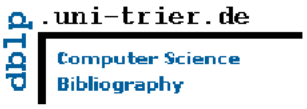

View my documents on
Scribd


BASE
Bielefeld Academic Search Engine


SCIRUS
search engine for science


SciRate.com


CiteSeerx beta


dblp .uni-trier.de
Computer Science
Bibliography


Q·Sensei


DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS


EBSCO
HOST


ProQuest

IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS
International Journal of Computer Science and Information Security (IJCSIS)
January-December 2013 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.
See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Cornell University Library, ScientificCommons, EBSCO, ProQuest and more.

Deadline: see web site
Notification: see web site
Revision: see web site
Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies
Digital information processing
Cognitive science and knowledge
Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site https://sites.google.com/site/ijcsis/

For more information, please visit the journal website (https://sites.google.com/site/ijcsis/)

Editorial
Message from Managing Editor

International Journal of Computer Science and Information Security *(IJCSIS – established since May 2009), is an online academic journal that adheres to robust peer review system and engages established and emerging scholars from several universities. The journal focuses on innovative developments, research challenges/solutions in computer science and information technologies. We are pleased to mention that we are committed to placing this journal at the forefront for the dissemination of novel and exciting research output and findings in the fields of computer science. Papers published in IJCSIS has received* ***enormous citations*** *and has been regarded as one of the best 3rd-tier Journal in the computer science research field.*

The goal is to bring together researchers and practitioners from academia and industry to focus on computer science issues and establishing new collaborations in these areas. Authors are solicited to contribute to this journal by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the Computer Science & Security. IJCSIS archives all publications in major academic/scientific databases; abstracting/indexing, editorial board and other important information are available online on homepage. Indexed by the following International agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest, EBSCO. Google Scholar reported a large amount of cited papers published in IJCSIS. IJCSIS supports the Open Access policy of distribution of published manuscripts, ensuring "free availability on the public Internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of [published] articles".

IJCSIS editorial board consisting of international experts solicits your contribution to the journal with your research papers, projects, surveying works and industrial experiences. IJCSIS appreciates all the insights and advice from authors and reviewers.

We look forward to your collaboration. For further questions please do not hesitate to contact us at ***ijcsiseditor@gmail.com****.*

A complete list of journals can be found at:
http://sites.google.com/site/ijcsis/

IJCSIS Vol. 11, No. 7, July 2013 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

TABLE OF CONTENTS

Analysis (PCA) and Fisher Linear Discriminant (FLD) are commonly used feature extraction methods for face recognition. In this paper, the focus is on perspective biometrics method based on facial and finger images using Scale Invariant Feature Transform. Image features generation transforms an image into a large collection of feature vectors, each of which is invariant to image translation, scaling, and rotation. It is useful due to its distinctiveness, which enables the correct match for keypoints between subjects. These features can be used to find distinctive objects in different images.

Keywords- SIFT, Biometric, Keypoints, Security, Person Identification, Scale invariant.

4. Paper 30061335: A Novel approach to provide 4 level High Security for the Mass of Cloud Data (pp. 18-24)

R. Balasubramanian, Manonmanium Sundaranar University, Tirunelveli, Tamilnadu, India.
Dr. M. Aramuthan, Perunthalaivar Kamarajar Institute of Eng.& Technology, Karaikal, Pondicherry,India

Abstract - In the world of Information Technology cloud computing is one of the emerging technologies. Cloud computing provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. When this cloud is made available for the general customer on pay per use basis, it has some security issues that must be considered during its deployment. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. Hence the primarily aim is to highlight the major high security issues existing in current cloud computing environments. Keeping in mind of the security required, this paper introduces a four level high security approach in the mass of cloud data. This new approach will give high security for the customer as well as the cloud storage service providers.

Key Words: Cloud Storage Service; Authentication; User Level Security; Data Level Security; Shared Level Security; Maintenance Level Security; Cloud server ; Service Provider.

5. Paper 30061336: Practical Routing Strategy in Delay-Tolerant Networks: A survey (pp. 25-30)

Lalitesh Kumar Choudhary, CSE, UIT, RGPV, Bhopal, India
Manish Kumar Ahirwar, CSE, UIT, RGPV, Bhopal, India
Uday Chaurasiya, CSE, UIT, RGPV, Bhopal, India

Abstract - A delay tolerant network is a special type of emerging network that experience frequent and intermittent connectivity or delays during communication. Also the delay tolerant network is a partition based network in which at any given time, the path between source and destination does not exist by which we may conclude that two nodes may never exist in a one connected portion of the network. As compared to conventional network the distinguishing feature can be summarized by two points i.e. Delay (Since there is no fixed connectivity and hence messages take time until they reach the destination) and resource constraints (Since all the nodes carry some limited buffer, it has to drop older messages if the buffer gets full in order to accommodate new messages). In this paper we have given emphasis on the various DTN routing approaches along with its pros and cons.

Keywords- Delay tolerant network; Knowledge Oracle; Custody Transfer

6. Paper 30061332: Design and Implementation of Multi Factor Mechanism for Secure Authentication System (pp. 32-37)

Khalid Waleed Hussein, Dr. Nor Fazlida Mohd. Sani, Professor Dr. Ramlan Mahmod, Dr. Mohd. Taufik Abdullah
Faculty Computer Science & IT, University Putra Malaysia (UPM), Kuala Lumpur, Malaysia

Abstract - A secure network depends in part on user authentication and regrettably the authentication systems currently in use are not completely safe. However, the user is not the only party that needs to be authenticated to ensure the security of transactions on the Internet. Existing OTP mechanism cannot guarantee reuse of user's account by an adversary, re-use stolen user's device which is used in the process of authentication, and non-repudiation.

This paper proposed mechanism of multi factor for secure electronic authentication. It intends to authenticate both of user and mobile device and guarantee non-repudiation, integrity of OTP from obtaining it by an adversary. The proposal can guarantee the user's credentials by ensuring the user's authenticity of identity and checking that the mobile device is in the right hands before sending the OTP to the user. This would require each user having a unique phone number and a unique mobile device (unique International Mobile Equipment Identity (IMEI)), in addition to an ID card number. By leveraging existing communication infrastructures, the mechanism would be able to guarantee the safety of electronic authentication, and to confirm that it demonstrates excellence in non-repudiation, authenticate user and mobile device which are used in the process of authentication, certification strength and also in comparison and analysis through experimenting with existing OTP mechanisms.

Keyword- Security, non-repudiation, multi factor authentication, IMEI.

Patterned & Protected AODV Against Black hole, Wormhole and Grey hole Attacks in convalescing Routing for Ad-hoc Network

Khyati Choure
PG-Scholar
DoCSE, OIST
Bhopal, India

Sanjay Sharma
Assistant Professor
DoCSE, OIST
Bhopal, India

***Abstract*—In this research work, AODV has been modified in such a way to improve its security feature. Obviously, performance has been improved in terms of Throughput and Packet Delivery Ratio, Avg, end-to-end Delay and Routing Overhead. A simulation has been performed to achieve better performance of modified New-AODV in presence of different attackers. Better results have been generated in terms of Throughput and Packet Delivery Ratio.**

Keywords: Throughput, End-To-End Delay, AODV, PDR, Routing Overhead, Attacks.

1. INTRODUCTION

1.1 Routing in Ad-hoc Network

The nodes in ad-hoc networks can be stationary or mobile; in the case of mobile they must cooperate with each other to enhance the performance of the network. The responsibility of the nodes is equal. Therefore, participating nodes on the network need to cooperate in order to establish routes and to forward packets to other nodes [3]. The nodes use routing protocols to establish and maintain the routes as shown in figure 1. The commonly used standard for ad-hoc networks is IEEE802. 11b, which is the standard for WLAN.

Packet Used in New-AODV

- **RREQ (Route Request):** Broadcasted for searching the shortest path
- **RREP (Route Reply):** Unicasted by destination for informing about the shortest path.
- **Data Packet:** Sent with the address of destination and on the shortest path.
- **RERR (Route Error):** Send by intermediate node on the failure of the forwarded path, If the node moves out of the network or it goes down then Route Error Packet (RERR) send back towards the source.
- **RREP-ACK:** For Reply ACK, This message is transmitted after successfully reception of data packet to the destination.

1.2 Attacks on AODV

In attacks on AODV, wrong routing information is generated by an attacker. For example, artificial route error messages (RERR) and routing updates may disturb the network operations or consume node resources. Some well-known attacks on AODV are described here:

Black hole attacks: A black hole is a malicious node that falsely replies for route requests without having an active route for the destination.

It exploits the routing protocol to advertise itself as having a good and valid path to a destination node. It tries to become an element of an active route, if there is a chance. It has bad intention of disrupting data packets being sent to the destination node or obstructing the route discovery process.

Wormhole attacks: In this type of attacks, the attacker disrupts routing by short-circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. However, generally, two or more attackers connect via a link called "wormhole link." they capture packets at one end and replay them at the other end using a private high-speed network.

Wormhole attacks are relatively easy to deploy but may cause great damage to the network.

Grey hole attack: Grey Hole is a node that can switch from behaving correctly to behaving like a black hole.

This is done to avoid detection. Some researchers discussed and proposed a solution to a grey hole attack by disabling the ability for intermediate nodes to reply to a Route Reply (RREP); only the destination is allowed to reply.

2. LITRATURE SURVEY

Work done by [7] can be appreciated in the field of Mobile ad-hoc network, which is also described how nodes communicated without a centralized mechanism in the network. The outcome of the algorithm [13] has a positive result in after simulating using ns-2.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

In AODV routing using MANET establish a single path for the communication [14] after handshaking process using RREQ & RREP. This paper introduces modified on-demand routing protocol [10] for MANET, which combines the performance metrics at each routing packet at each node. To the extension of the RREQ / RREP packet [11] provide more efficient multi-path routes. The outcome of this research has a higher packet delivery ratio and lower routing packets.

Research has been contributed in [12]. Ad-hoc networks are characterized by multi-hop wireless connectivity and frequently changing network topology, which have made it infrastructure less [9].

This Research has been contributed in an Ad-hoc network is the collection of mobile nodes [3] communicating without a centralized infrastructure. MANET generally uses a wireless [5] radio communication channel. So they are open to various types of attack. The outcome of this research performance [4] of AODV is improved in the presence of attack. Future direction of the research is looking for the solution of other kinds of attack.

This Research has been contributed in. In MANET, routers have recreated many times due to the mobility of the nodes. If a node in a mobile ad-hoc network [1] aware of the mobility of the neighbour nodes, then highly mobile node is to avoid becoming a part of routes, this will greatly reduce new path discovery towards the destination.

3. PROPOSED WORK AND ALGORITHM

3.1 Proposed Work

In this work, a modification has been proposed in REEQ and RREP-ACK field of AODV [14] and one extra field "Security Guard." has also been added in the existing field to improve security in AODV.

In existing work [11] it has been found that 1 bit has been modified (0 to 1) in the RERR frame format to convert it into PRERR, and this modified bit included priority information regarding multiple link failures.

In our proposed work, we have enabled another single bit of RERR frame format, which will store security information. Node Tribute History, Type of attacker, and finally including or excluding information about the attacker is included in this bit.

In this approach, some logics have been developed to find true attackers using delay and Tribute history on each node.

3.2 Proposed Algorithm

Step 1: Initialize Tribute Value of each node (Say N)

Step 2: Broadcasted RREQ message to discover a route and decrease the Tribute Value (CV) of each node by -1, (**CV= N-1)**

Step 3: If RREQ message is received by destination, then shortest path is made available by unicasting a RREP back to the source route.

Step 4: Source node will send Data Packet to the Destination node using the shortest path.

Step 5: If RREP-ACK is received, then increase Tribute Value of each node in the shortest path by +2 and Go to step 8.

Else apply the local route repair mechanism to recover the route.

Step 6: If a route is available after local route repair, then sends a data packet through repaired path and Go to step 8.

Else forward data packet to next to next node and wait for RREP-ACK.

Step 7: If RREP-ACK is received, then send it to the source node.

Else Go to step 8.

Step 8: Observed the Tribute value of each node in the shortest path.

Step 9: If the Tribute value is <= (N-10), then declare the node as Bad node and calculate the PDR of each node.

Step 10: If PDR = 0, or Data Packet Flow=0 or then declare the node as a black hole attacker.

Step 11: If 0 < PDR < 0.2, then declare the node as a grey hole attacker nodes.

Step 12: If 0.2 < PDR < = 1, and delayed by more than Avg. End-to-end delay (Calculated based on RREP-ACK time of each packet), declare the node as a warm hole attacker node.

3.3 Results of simulation have been analyzed based on the following parameters.

3.3.1 End-to-end delay: It is the total average time taken for a packet to be transmitted across a network from source to destination.

3.3.2 Routing Overhead: It refers to the control packet count(RREQ, RREP and RERR) to send the data packet in the network for routing information sent, which uses a portion of the available bandwidth of a communications

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

protocol. These extra control packets are referred to as routing overhead, since it does not contribute to the content of the data packet or message.

3.3.3 Throughput: No. of packet transmitted per unit of time.

If Successfully Transmitted Packets=Pt., and time taken to do it is t, then.

$$Pth = P_T/t \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

3.3.4 Packet Delivery Ratio

It is defined as the ratio of packets received to packet transmitted, generally represented in percentages. If Packet Transmitted=P_t, and Packet received is P_r, Then.

$$PDR\ (\%) = P_r/P_t * 100 \ldots\ldots\ldots\ldots (2)$$

Transmitter Range	**300 m**
Bandwidth	**2Mbits/s**
Simulation Time	**110**
Number of nodes	**10,20,30, 40, 50**
Scenario size	**500 x 500 m2**
Traffic type	**CBR(Constant Bit Rate)**
Packet size	**64 bytes**
Rate	**20 packets/s**
Initial Energy	**50**
Model	**Random wave Point**
Packet Size	**512 Bytes**
Simulation Time	**120 Second**

Table 1: Simulation Environments

3.4 Results Analysis

Based on simulation using NS-2.34 [17] results has been evaluated and compared with AODV using four well known parameters, i.e. Throughput, Packet Delivery Ratio, End-to-End Delay, Overhead.

3.4.1 Throughput In presence of Attacker

Figure 1 shows improvement in New AODV in terms of Throughputs when attacker nodes [16] are presented in the Network.

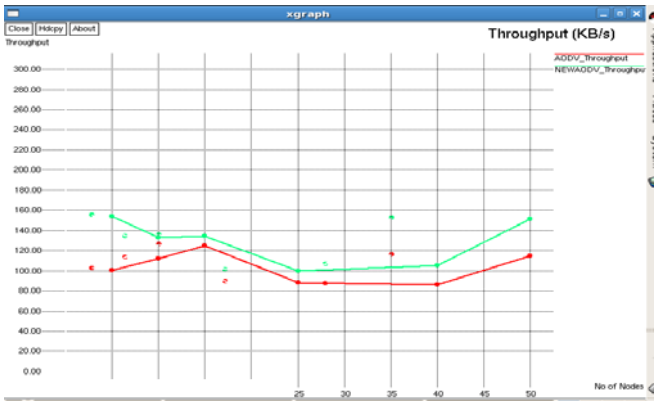


Figure 1: Throughput with Attack

It can be seen that Throughput is always greater in case of New AODV, because of identification and discarding of attackers on the bases of packet dropping behavior of attacker by black whole attack.

3.4.2 PDR (Packet Delivery Ratio) with attack

It can be seen the Figure 4 that PDR is increases whenever we use New-AODV. Attackers [15] identified and discarded so received packets increases because of reduction in packet dropping by attackers using Black whole attack.

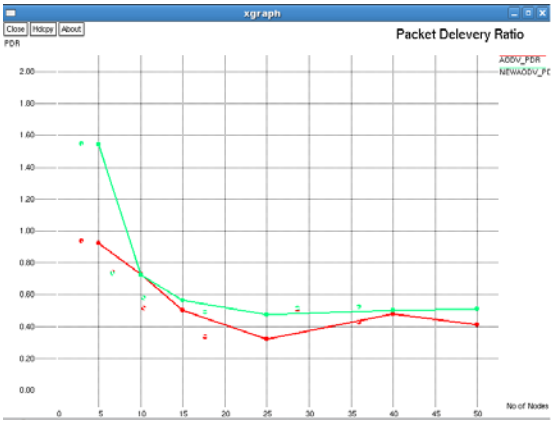


Figure 2: PDR with Attacks

Performance of New AODV is better in case of low nodes. When nodes increase performance degraded because of obvious congestion in the networks, but still it is better than AODV.

3.4.3: No. of Attacker Detected

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

It can be seen the Figure 3 that No. of attacker can be detected and identified as Grey hole, worm hole and Black hole Attackers.

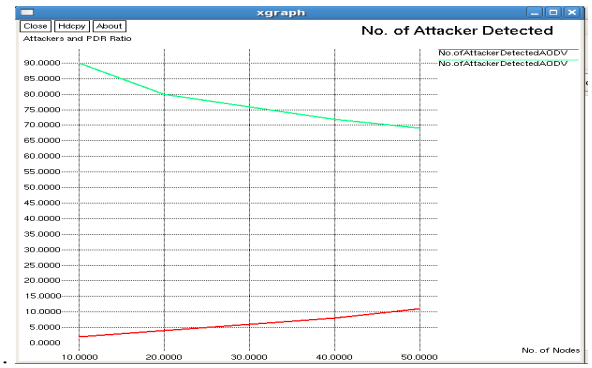


Figure 3: Attacker Nodes Detected

It can be observed that in presence of attacker's performance of AODV is degraded as compared to without attack case because the attacker always harmed the networks.

3.4.4 Avg. End-to-End Delay with Attack

It can be seen in Figure 4 that Average End-to-End Delay is increases whenever we use New AODV because of using prioritized control packet to inform other nodes as early as possible about congestions. In every research work, there is some benefit and some loses this is a drawback of this research work. Congestion also increases because of presence of attacker nodes in the networks.

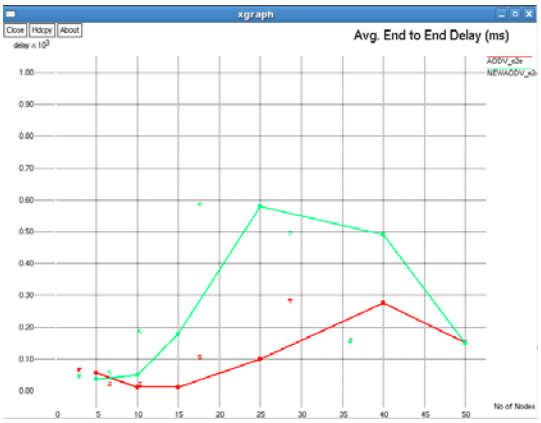


Figure: 4 Avg. End-To-End Delays with Attack

It can be easily observed that at low loads, this delay is small in case of New AODV and AODV but whenever we increase the number of nodes, these delay increases and difference between both the protocols become wider than at its low values.

3.4.5: Attacker Type Classifications.

Attacker types can be classified using different PDR values.

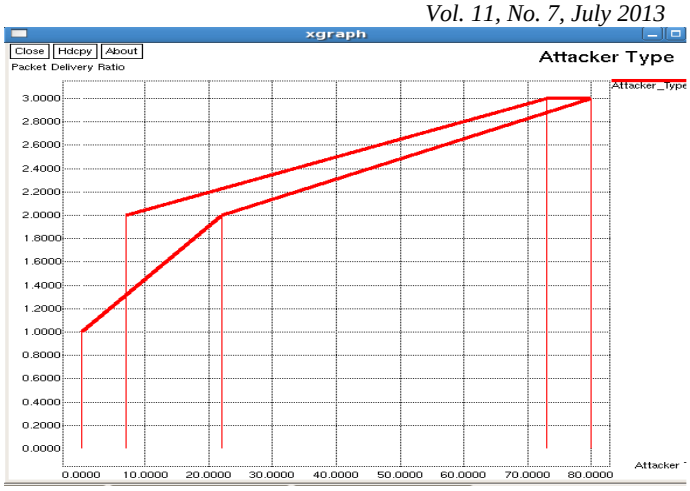


Figure 5: Attacker Nodes Detected

4. CONCLUSION & FUTUTRE WORK

In this work, some modification have been done normal working of standard AODV protocol for enhancement of performance of routing process for Mobile ad-hoc Networks. It can be seen that improvement in throughput have been observed. Tribute count and delay involve and PDR (Packet Dropping Ratio) increases because of reduction in packet dropping by attackers. Performance of Modified-AODV is better in case of all types of nodes in the networks.

In future modified AODV can be applied in VANET.

References

[1] Wang Nanning, Cao Yemen "Improved AODV protocol with Lower Route Cost and Smaller Delay "IEEE Fourth International Conference on Intelligent Computation Technology and Automation 15 April 2011 pp7-11

[2] Habib-ur Rehman, Lars Wolf "Performance Enhancement in AODV with Accessibility Prediction" IEEE International conference on sensor network 12 JAN 2008 pp. 1-6

[3] Nandkumar Kulkarni, Ramjee Prasad1, Horia Cornean, Nisha Gupta" Performance Evaluation of AODV, DSDV & DSR for Quasi Random Deployment of Sensor Nodes in Wireless Sensor Networks" IEEE International conference on Devices and communication25 FEB 2011 pp. 1-5

[4] Sung-Ju Lee and Mario Gerla "AODV-BR: Backup Routing in Ad hoc Networks" IEEE, JAN 2000, PP 1311-1316

[5] Azzedine Boukerche,"A Simulation Based Study of On-Demand Routing Protocols for Ad hoc Wireless Networks" IEEE, JAN 2008, PP 85-93

[6] Neda Moghim "An Improvement On Ad-hoc Wireless Network Routing Based On AODV", 8th International Conference Communication Systems, 2002. ICCS 2002 25-28 Nov. 2002, PP 1068 - 1070 Vol. 2

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[7] Q. Wang "A Robust Routing Protocol For Wireless Mobile Ad-Hoc Networks", The 8th International Conference on Communication Systems, 25-28Nov 2002, pp 1071 - 1075 Vol. 2

[8] HAO Zhang," Analysis of Two Ad Hoc Broadcasting Protocols", American Control Conference, 2004. PP 3599-3604, Vol. 4

[9] Jin-Man Kim "A Performance Evaluate of Improved AODV-Based Power-Aware Routing Protocol in MANET". Proceedings of 7th International Workshop on Enterprise networking and computing in Healthcare Industry, 2005. HEALTHCOM2005, 23-25 June 2005, pp 273 - 277

[10] Yusuke "AODV Multipath Extension uses Source Route Lists with Optimized Route Establishment", 2004 International Workshop on Wireless Ad-Hoc Networks, 31 May-3 June 2004, pp 63 - 67

[11] Vahid Nazari Talooki, "Performance Comparison of Routing Protocols for Mobile Ad-hoc Networks", Asia-Pacific Conference on Communications, 2006. APCC '06. Aug. 31 2006-Sept. 1 2006, pp. 1 - 5

[12] Cao Minh Trang "A Distributed Intrusion Detection System for AODV" Asia-Pacific Conference on Communications, 2006. APCC '06, Aug. 31 2006-Sept. 1 2006, pp 1 – 4

[13] Hussain S.A, Garcia, E, Idrees, M." Throughput Enhancement in AODV Routing Using Mobility Awareness", 9th International Multi topic Conference, IEEE INMIC 2005, July 2005, pp. 1-4

[14] Jagpreet Singh, Paramjeet Singh, Shaveta Rani, "Enhanced Local Repair AODV(ELRAODV)," International Conference on Advances in Computing, Contro and Telicommunication Technologies, IEEE Conmputer Society, pp. 787-791, 2009.

[15] Umang Singh, B. V. R. Reddy, M. N. Hoda,"GNDA: Detecting good neighbor nodes in ad-hoc routing protocol," Second International conference of Emerging Trend in Information Tehcnology, pp.235-238, 2011.

[16] Vikash Solomon,"Survey of Attacks on Mobile Ad-hoc Wireless Networks," International Journal of Computer Science & Engineering , Volume. 3, No.2, pp. 826-829 Feb, 2011.

[17] Network Simulator N.S-2 Documentation: www.isi.edu/nsnam/ns/ns-documentation.htm.

khyati choure is M.Tech scholar in the Department of Computer Science & Engineering,Oriental Institute of Science & Technology,Bhopal. Her research interest lies in Ad hoc network

Rule Based Approach for Keystroke Biometrics to identify authenticated user

Kulwinder Singh
Department of Computer Science and Engineering
Lovely Professional University
Jalandhar, Punjab, India
kulwinder.padda143@gmail.com

Harjeet Kaur
Department of Computer Science and Engineering
Lovely Professional University
Jalandhar, Punjab, India
harjeetkaurminhas@gmail.com

Abstract— **Advancement in the field of Information Technology makes information security is an inseparable part of it. Biometric technologies are very reliable for providing authentication and verification. So, in order to deal with security, Authentication plays an important role. This paper investigates the study of keystroke dynamics to identify individuals based on their typing rhythm behavior with the help of fuzzy rule based system. Identification of the user becomes more accurate with the use of Neighbor Key Pattern, Which will help to differentiate between the imposter and legitimate user. The User Type has been identified on the basis of some critical keystroke factors. This approach makes use of the inter-stroke gap that exists between consecutive characters of the user identification. With the use of behavioral traits such as typing rhythm of different users more accurate results are analyzed. However, the quality of the user's patterns of behavior based biometric can be improved by increasing the peculiarity of the typing style.**

Keywords- **Authentication; Biometrics; Fuzzy Logic; Keystroke Dynamics; Computer Security.**

I. INTRODUCTION

There are so many ways to secure our system from the Cyber Attack. Username and password pairs are used as authentication factors to logged into the account. In a secure system, all accounts must either have passwords or be invalidated. Username and password have been and still are the main method to gain access to computers. The stand-alone computer is not connected to the Internet or a local or wide area network, so to secure the data we need to emphasize on the password based security. The current access systems prompt users to authenticate themselves with a username and password means the users need to type their respective Username and Password to Login. This method of authentication relies on the password's secrecy and, and also in some cases the username's secrecy. If this secrecy is not breached, then the statement is that these tokens are able to uniquely identify a valid user.

Keystroke dynamics is the term given to the procedure of measuring and assessing a user's typing style. These measures, based largely on the timing latencies between keystrokes, are compared to a user profile as part of a classification procedure; a match or a non-match can be used to decide whether or not the user is authenticated, or whether or not the user is the true author of a typed sequence. [4]. User Authentication can be categorized as follows [6][11].

- Object based user
- Knowledge based
- Biometric based

The "Object-based" authentication relies on Voiceprint; traditional keys to the doors can be assigned. Usually the token-based approach is combined with the knowledge based approach. In "Knowledge-based" user authentication the user is asked to answer at least one "secret" question. Secret questions can be static or dynamic [6].

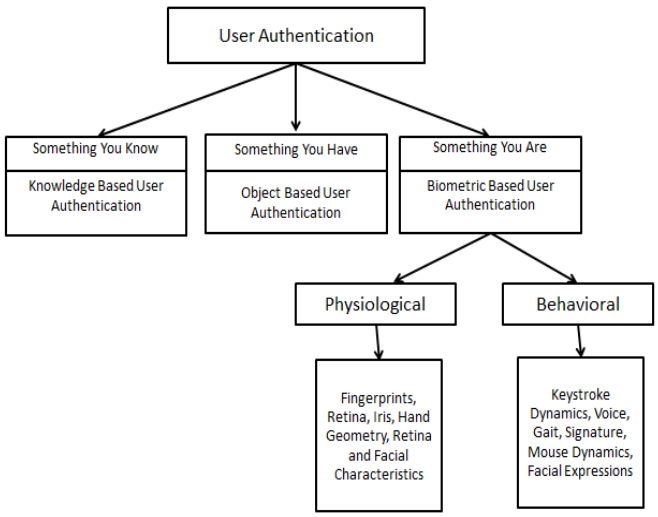


Figure 1: Approaches of user authentication

With the use of rule based keystroke biometric into the existing password authentication systems, even if the imposter enters the correct login credentials and try to breach passwords either they use different hacking mechanism, Key logger or shoulder spoofing with or without the right attempt pattern they will be denied access because in this rule based biometric system user authentication depends upon the critical typing behavior factors.

II. BACKGROUND STUDY

Due to the increasing importance of cyber security keystroke dynamics has become an active research area. Keystroke dynamics features are usually extracted using the timing information of the key down/hold/up events. Killourhy K. *et al*., develop an evaluation procedure, and measure the performance of many anomaly detection algorithms on an equal basis. . In the process, established which detectors have the lowest error rates and provide a data set and evaluation methodology that can be used by the community to assess new detectors and report comparative results [5][1]. Maxion R. *et al*., Keystroke dynamics most of the researchers have explored the domain by using the Number Pad input in which," 28 users typed the same IO-digit number, using only the right-hand index finger and achieved an unweight correct-detection rate of 99. 97% with a corresponding false-alarm rate of 1.51%, using practiced 2- of-3 encore typing with outlier handling [14].

The password problem arises in the conventional security systems because the mechanism was that Passwords should be easy to remember. Passwords should be secure means they should look random and they should be changed frequently so that should be hard to guess [6] [10]. Matching functions such as Gaussian Probability Density Function (GPD) and Direction Similarity Measure (DSM) with different fusion approaches such as Single Layer Single Expert (SLSE) with EER (14.87%), Single Layer Multiple Expert (SLME) with EER (2.791%) and Multiple Layer Multiple Expert (MLME) with EER (3.733%) are used to combine scores from different methods [4].

Development of a common nomenclature for the features will possibly clear the ambiguity present in describing features and help in accurate comparison of feature by the research on effective size and type of passwords and the number of samples needed for a person to enroll and authenticate should be conducted so that users can be enrolled and authenticated as quickly as possible [3].

III. PROBLEM AND APPROACH

The password problem arises in the conventional security systems because the mechanism was that Passwords should be easy to remember. Passwords should be secure means they should look random and they should be changed frequently so that should be hard to guess [6] [10].

To make measurable progress in the field of keystroke dynamics, shared data and shared evaluation methods are necessary. The methodology used in which timing data collected and used to identify the user is authenticated or not. There are two phases i.e. Enrolment Phase and Verification Phase.

Enrollment Phase— The enrollment step allows creating the model of each user and also the enrolled sample. During this phase the key pressure and timing pattern would be stored along with the unique password in the database. Features extracted from the raw typing data i.e. Latency Keystroke Latency such as press-to-press (PP), release-to-release (RR) and release-to-press (RP) latencies [4] [15]. The training set is collected, and a template is created containing the patterns found in it. User's typing pattern will be stored in the database, which will contain actual key pressed, neighbor key pressed and wrong key pressed along with the total and average time to enter the password.

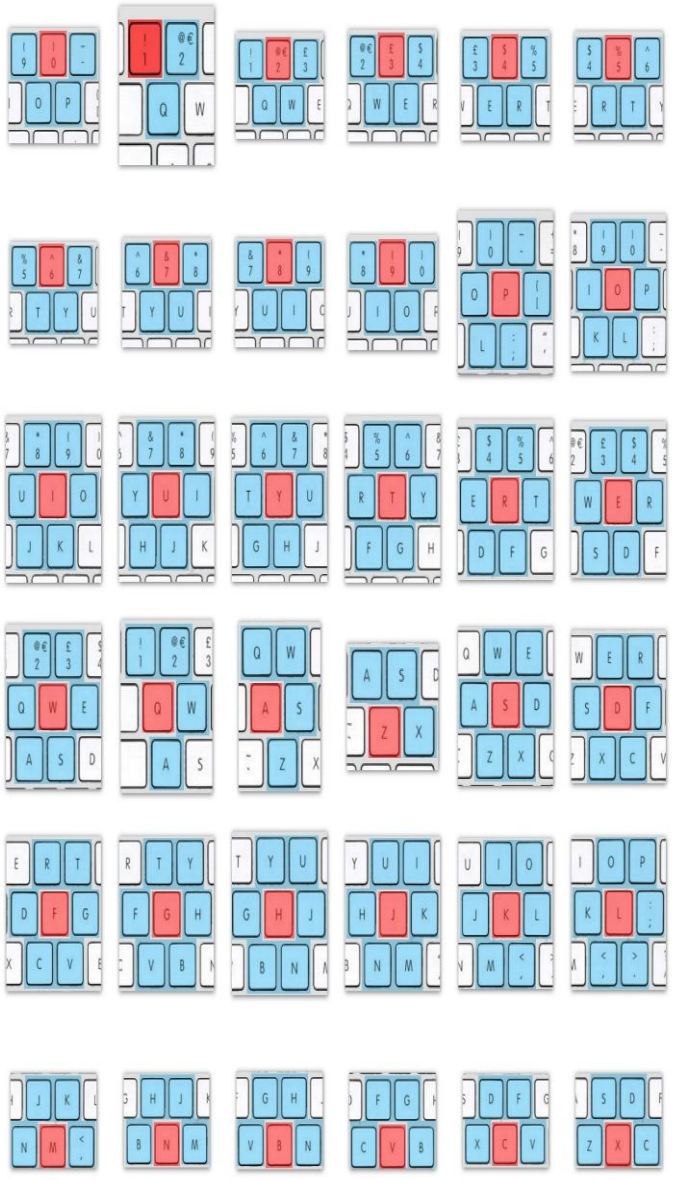


Figure 2: Standard Keyboard neighbor key patterns for Keystroke Biometrics

The raw measurements used for keystroke dynamics are dwell time and flight time.

Dwell time - The time duration that a key is pressed and the user holds down a key.

Flight time - The time duration in between releasing a key and pressing the next key.

When a user type a series of characters, at that time the subject needs to find the right key which is specific to that subject [14] [4].

Several different measurements can be detected when user presses the keys on keyboard are as follows:

- Password Length.
- Attempt Pattern will be stored in database.
- Actual total time taken to enter the password.
- Attempt total time taken to enter the password.
- Actual average time to enter the whole password.
- Attempt average time to enter the password.
- Total time deviation from the current/actual password.
- Attempt average time deviation from the current/actual password
- No. of trials will be given on the basis of key pressed.

Verification Phase— In the verification phase the input of the user corresponds to the claimed identity will be verified. The way of capturing these inputs greatly depends on the kind of used keystroke dynamics system. While user will type the timing information will be captured if sample is false again then the user is considered an impostor.

The Static verification approaches analyze keystroke verification characteristics only at specific times providing additional security than the traditional username/password. For example, during the user login sequence Static approaches provide more robust user verification than simple passwords but the detection of a user change after the login authentication is impossible [8]. Continuous verification, on contrary, monitors the user's typing behavior throughout the course of the interaction. In the continuous process, the user is monitored on a regular basis throughout the time he/she is typing on the keyboard, allowing a real time analysis [7] [8].

The purpose of the proposed system is to provide no. attempts based upon keyboard patterns i.e. if a button is pressed which is neighbor of the required character then the no. of attempts to re-enter the login credentials will not be reduced. On the other hand if the key pressed is far away from the target key then the no. of attempts will be reduced. As the standard neighbor key pattern so accordingly the attempt patterns generated.

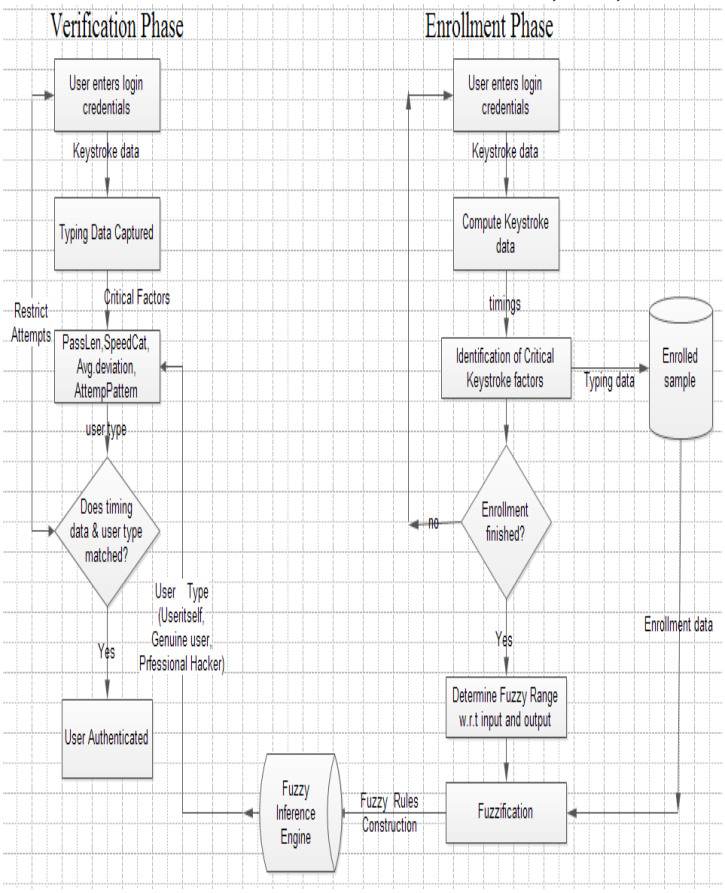


Figure 3: Password based authentication scenario of the rule based system

IV. FUZZY RULE BASED APPROACH FOR KEYSTROKE BIOMETRICS

The process of Rule based keystroke biometrics starts with the identification of those critical factors, which directly or indirectly influenced user's typing behavior while the user enter the login credentials. After deciding those factors, set up the values for those parameters. Providing values to some of these parameters sometimes may be a tedious task, in that case an interface used that has been designed to get the typing rhythm data. Values for different keystroke parameters are stored in the fact base (or working memory). Further, parameters are then fuzzified and creates a fuzzy knowledge base, which is basically a collection of fuzzy rules.

Fuzzification process will be started in which all the crisp values provided with the input variables will be transformed to the fuzzy values and for all the inputs respective rules will be generated. Then those fuzzy rules are process on the facts in the working memory in the fuzzy inference engine by applying any fuzzification method [13][16][17]. At the end the outcome of the fuzzy inference engine are defuzzified to provide the identity of the user i.e. User itself, May be Genuine User or Professional Hacker.

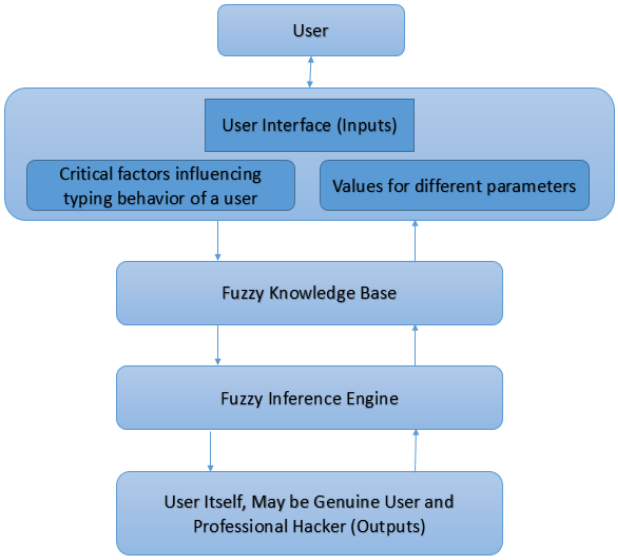


Figure 4: Rule based keystroke biometric working process

V. FUZZY RULE BASE INFERENCE ENGINE PROCESS FOR KEYSTROKE DYAMICS

Step 1: Identification of critical Keystroke factors

Different parameters that are introduced above are used acquired the required knowledge of users' typing behavior. Critical factors that are used to provide input to the fuzzy knowledge base are:

Password Length-- It will contain the total no. of characters that are typed by the user.

Speed Category-- The total time and average time to enter the password is being calculated in milliseconds. Speed category will be decided on the basis of average time taken by the user like very slow, slow, fast and very fast.

Average Deviation-- As in the enrolment phase while user register for an account the total time will be stored in the database. From that the average time will be calculated as:

$$Average\ time = (Total\ Time/Password\ Length) \quad (1)$$

These are the Actual values or we can say the original Total time and Average Time Values. Now, at the time of Login there will be another Total time and Average time will be stored in database i.e. the Attempt total time and Attempt average time. So the Average deviation time can be calculate from here as:

$$Average\ Deviation = (Attempt\ average\ time - Actual\ average\ time) \quad (2)$$

Based on this factors the user's typing rhythm difference can be calculated which will help to identify the average deviation between the typing rhythms while the user enter Login credentials.

Attempt Pattern- The most important and considerable factor is the attempt pattern, which includes the Exact key pressed, the neighbor key pressed and the wrong key pressed pattern. This pattern will be very helpful to identify the user type, whether the person is the legitimate user or not. Because if the exact key pressed or in case a neighbor keys of the password pressed then it can be considered that user haven't type this intentionally. Suppose if the password is (im@Xping7) the no. of characters in this password are 9, so if the user enter the correct password then it will return attempt pattern as 111111111. Now, in case user missed the exact character there will be more chances of pressing the Neighbor key, so that will return some pattern like 112111112 in this case it is clear that there will be two neighbor keys pressed so the number of attempt will be gradually decreased. The third case will be that if in case user pressed a wrong key and also some of the neighbor keys then that will not be considered as the legitimate user such as the attempt pattern will be like 110011221. So the number of attempt provided to a user will be instantly reduced.

Step 2: Fuzzification

This phase involves the designing of the fuzzy expert system for the Keystroke Dynamics. In this phase, input and output variables are defined. Here fuzzy sets are defined and the input is fuzzified with the help of defined membership function [16] [17].

TABLE 1. Input and Output variables for Keystroke Dynamics

Factors	Fuzzy Input Variables and their Memberships range				Fuzzy Output Variables and their memberships range		
	Low	Medium	High	Very High	User Itself	May be Genuine user	Professional Hacker
Password Length	1-2	2-4	4-6	6-10	1-3	3-6	6-10
Speed Category	1-100	101-200	201-500	501-800			
Average Deviation	-200-0	-50-250	200-600	550-1000			
Attempt Pattern	0.8-1.2	1.2-2.8	2.8-3.2	3.2-4.0			

In this table the fuzzy input variables have given the range and for these values there will be some respective output values that ranges are set for the output variables. The unit of time taken is *millisecond (ms).*

Step 3: Fuzzy Rule Construction

The knowledge base of the fuzzy rule based system stores knowledge in the form of the rule and draw inference by using these rules. So for engineering the knowledge base, the formation of rules take place. The rule in the fuzzy system is in simple if-then statements.

Step 4: Fuzzy Inference Rule generation

These if-then rule statements are used to formulate the conditional statements that is a part of fuzzy logic [13] [16].

IF: Condition-1 and Condition-2 and Condition-3 Condition-4
THEN: Take Action-4

The knowledge base of this system i.e. rule based system for keystroke dynamics contains 192 rules. Some of the rules are as follows:

- *If (Password_Length is low) and (Speed_Category is low) and (Average_Deviation is low) and (Attempt_Pattern is low) then (User Type is User itself).*
- *If (Password_Length is low) and (Speed_Category is Medium) and (Average_Deviation is low) and (Attempt_Pattern is Medium) then (User Type is May be Genuine).*
- *If (Password_Length is low) and (Speed_Category is low) and (Average_Deviation is Medium) and (Attempt_Pattern is high) then (User Type is Professional Hacker).*
- *If (Password_Length is low) and (Speed_Category is medium) and (Average_Deviation is high) and (Attempt_Pattern is Medium) then (User Type is May be Genuine)*

VI. Experimental Results

In this paper, four critical keystroke factors are analyzed in our classifier to authenticate the identities of the users. At first the critical factors identified for Typing Behavior are considered as inputs for the fuzzy inference system and are represented in the form of fuzzy linguistic variables with their member elements. Then each variable is assigned with fuzzy membership using triangular membership functions.

The membership function for Average Deviation has four fuzzy sets low, medium, high, very high. The membership function used in this system is the triangular membership function. It is also necessary to set the range for output membership function accordingly. Similarly for the other input variables membership function have been defined.

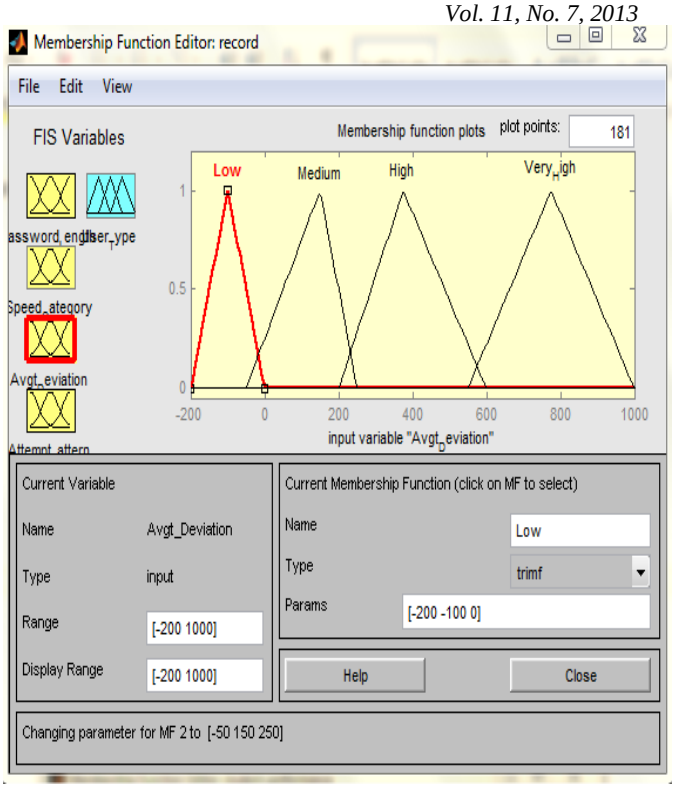


Figure 5: Membership Function Editor for Average Deviation

Following is the figure that shows the membership functions of the output variables.

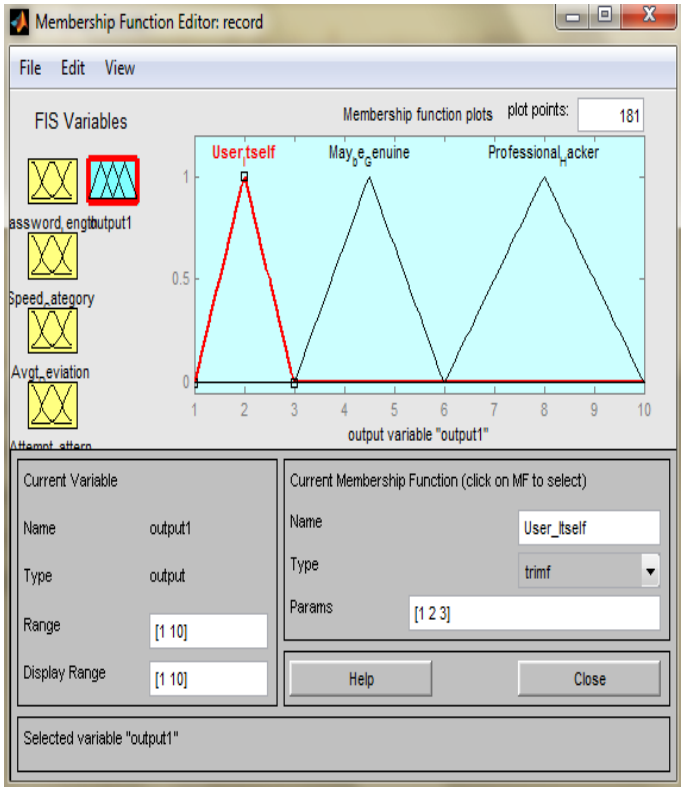


Figure 6: Membership Function Editor for Output User Type

When the membership functions are selected, rule editor is used for generating rules. In Fuzzy Inference Systems, based on the template keystroke data provided by the different users, decisions are made and outputs are generated.

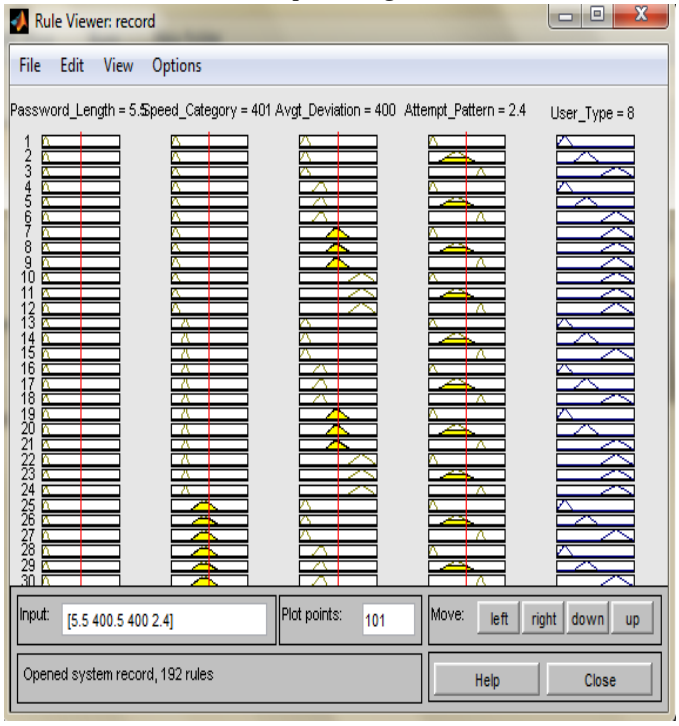


Figure 7: Fuzzy rule generation of Keystroke Biometric System

Using the Surface Viewer, a three-dimensional curve can be viewed that represents the mapping from two inputs and one output.

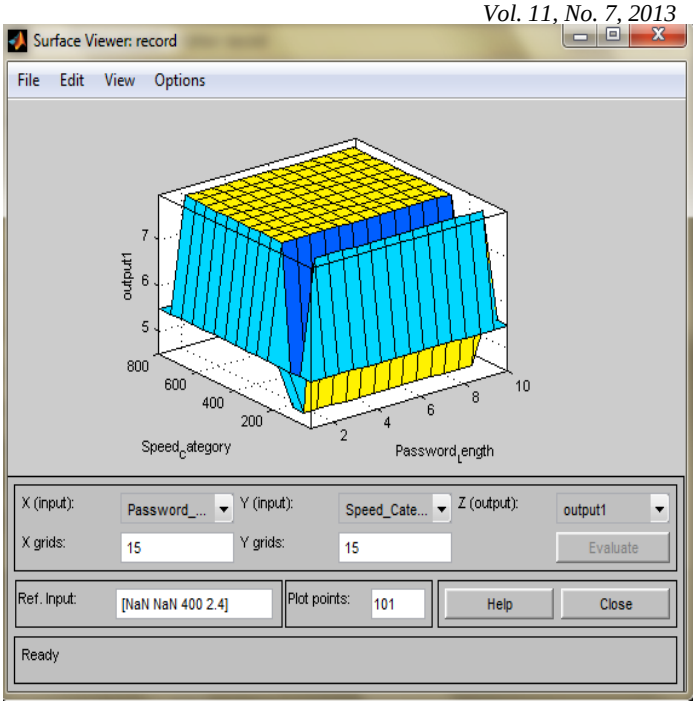


Figure 8: Surface viewer of Rule based Keystroke Biometric

Surface viewer used the inputs password length, Speed category and the output is User Type.

The system is tested by using different defuzzification techniques. System is defuzzified on Centroid method, Bisector, SOM, LOM, MOM to test the robustness of the rules and knowledge engineering of tool.

TABLE 2. Defuzzified values of using different approaches

Password Length (1:10)	Speed Category (1: 800)	Average Deviation (-200:1000)	Attempt Pattern (0.8:3.8)	Defuzzified Values of User Type (User Itself / May be Genuine User/ Professional Hacker)									
				Centroid		Bisector		Mom		Lom		Som	
				Values	Rank	Values	Rank	Values	Rank	Values	Rank	Values	Rank
9	3	385.87	1	7.997	1	8.02	1	8.02	1	9.91	1	6.13	1
9	3	-103.22	1	2.012	3	1.99	3	1.99	3	2.89	3	1.09	3
4	2	-54.619	1	5.5	2	5.5	2	5.5	2	5.5	2	5.5	2
7	3	136.69	1.142	2.012	3	1.99	3	1.99	3	2.89	3	1.09	3
9	3	211.72	1.142	5.5	2	5.5	2	5.5	2	5.5	2	5.5	2
6	2	435.56	1.142	7.997	1	8.02	1	8.02	1	9.91	1	6.13	1
4	2	141.91	1	2.0126	3	1.99	3	1.99	3	2.89	3	1.09	3
7	3	252.53	1	2.0126	3	1.99	3	1.99	3	2.89	3	1.09	3
3	1	-106.03	1	5.5	2	5.5	2	5.5	2	5.5	2	5.5	2
9	3	-75.121	1	2.0126	3	1.99	3	1.99	3	2.89	3	1.09	3
7	2	278.14	1.285	7.975	1	8.02	1	8.02	1	9.91	1	6.13	1
2	3	-44	1	5.5	2	5.5	2	5.5	2	5.5	2	5.5	2
7	3	278.14	1.285	7.975	1	8.02	1	8.02	1	9.91	1	6.13	1

VII. Error Metrics

The Error metrics such as False acceptance rate and False rejection Rate are calculate for the proposed system which are determining the performance of rule based keystroke biometric authentication system [3] [18] [19].

FAR is the percentage of imposters that are inaccurately allowed as genuine users.

$$FAR = \frac{Number\ of\ false\ matches}{Total\ number\ of\ impostor\ match\ attempts}$$

FRR is the number of genuine users rejected from using the system. It is defined as:

$$FRR = \frac{Number\ of\ false\ rejections}{Total\ number\ of\ genuine\ match\ attempts}$$

Also it is find out the overall system accuracy is 85.71% as with the data collection of total 11 typists and with the error metrics of FAR= 0.146 and FRR= 0.241. The system is more reliable and accurate to identify the imposter and legitimate user. There are some factors that affect the false rejection rate such as tiredness and some other factors. So the overall system is accurate in accordance with performance and reliability. So, we are getting the same result by using different defuzzification techniques. This also shows that the system which is developed is Robust.

TABLE 3. Calculation of FAR and FRR

Participant	False Rejection Rate (FRR)	False Acceptance rate (FAR)
1	0.210	0.181
2	0.333	0.177
3	0.375	0.125
4	0.285	0.111
5	0.363	0.051
6	0.140	0.20
7	0.360	0.121
8	0.230	0.480
9	0.090	0.18
10	0.153	0.112
11	0.121	0.051
Total	2.66	1.609
Average	0.241	0.146

VIII. Conclusions and Future scope

The fuzzy rule based System for Keystroke dynamics shows the future of biometric technologies is promising. In this system there are several factors that are analyzed for the identification of imposter and legitimate user. The rule based system will also restrict the number of attempts of the users so it can be a better biometric as there are some certain amount of attempts. Moreover, the increase in accuracy using the fuzzy rule base plays a big part in the field of Keystroke biometrics. Identification of the imposter also becomes easier as the neighbor key pattern introduced in this. Also the identification rate of the overall system makes this system more reliable. On the other hand, As Keystroke Dynamics is the cheapest form of biometric so it is more reliable to use. There are still some set of challenges in this field that need to be overcome in order for it to become an effective Biometric. So it have the enormous potential to grow in the field of Cyber Security. In future this fuzzy rule based system can be made more accurate in

performance so that no legitimate user can be considered as an imposter. As Mobile devices are increasing in popularity so this approach can be applied there in the near future. However, this rule based approach has enormous potential to arise in the area of cyber-security. Also in the field of remote monitoring keystroke dynamics can be used since it is non-intrusive and a cost-effective biometric.

REFERENCES

[1] Killourhy, K. S. (January, 2012). "*A Scientific Understanding of Keystroke Dynamics.*" Pittsburgh, PA 15213.

[2] Yu Zhong, Y. D. (2012). Keystroke Dynamics for User Authentication . *Non-Technical Data - Releasable to Foreign Persons.* .

[3] Salil P. Banerjee, D. L. (July 1,2012). Biometric Authentication and Identification using Keystroke: A Survey. *Journal of Pattern Recognition Research*, 116-139.

[4] Pin Shen Teh, S. Y. (2012). Feature Fusion Approach on Keystroke Dynamics Efficiency Enhancement . *International Journal of Cyber Security and Digital Forensics(IJCSDF)*, 20-31.

[5] Kevin S. Killourhy, R. A. (2009). Comparing Anomaly-Detection Algorithms for Keystroke Dynamics.

[6] Mrs. D. Shanmugapriya, D. G. (2009). *"A Survey of Biometric keystroke Dynamics:"*. International Journal of Computer Science and Information Security , II, 115-119.

[7] Fabian Monrose, M. K. (2000). "Password Hardening Based on Keystroke Dynamics. acm" , 1-10.

[8] Patrick Bours, H. B. (2009). *"Continuous Authentication using Biometric Keystroke Dynamics"*. The Norwegian Information Security Conference, (pp. 1-12).

[9] Peacock, A., Ke, X., & Wilkerson, M. (2004). *"Typing patterns: A key to user identification."* Security & Privacy, IEEE, 2(5), 40-47.

[10] Sally Dafaallah Abualgasim, I. O. (2011). *"An Application of the Keystroke Dynamics Biometric for Securing PINs and Passwords."* World of Computer Science and Information Technology Journal (WCSIT) , 1(9), 398-404.

[11] Preet Inder Singh. (2012, april). *"Enhanced Password Based Security System"*. I.J. Information Engineering and Electronic Business , 30-35.

[12] Kiran S. Balagani a, V. V. (2011). "On the discriminability of keystroke feature vectors used in fixed text." Elsevier , 32, 1070-1080.

[13] Ross T. J. (2005). "Fuzzy logic with engineering applications." John Wiley & Sons.

[14] Roy A. Maxion, K. S. (2010). *"Keystroke Biometrics with Number-Pad Input."* International Conference on Dependable Systems & Networks (DSN) , 201-210.

[15] Deian Stefan, D. (. (2010). Keystroke-Dynamics Authentication Against Synthetic Forgeries. IEEE , 1-8.

[16] Fasanghari M., Montazer G. A. (2010). "Design and implementation of fuzzy expert system for Tehran Stock Exchange portfolio recommendation, Expert Systems with Applications," 37, 6138-6147.

[17] Matthews C. (2003). "A formal specification for a fuzzy expert system, Information and Software Technology", 45, 419–429.

[18] Ting-Yi Chang, C.-J. T.-J.-C. (2011). *"User Authentication using Rhythm Click Characteristics for Non-Keyboard devices"*. IACSIT,IPCBEE , vol.13, 167-171.

[19] Damon L. Woodard, B. M. (2004). "EXPLOITING FINGER SURFACE AS A BIOMETRIC IDENTIFIER".

AUTHORS PROFILE

Kulwinder Singh B.Tech (CSE,2012), M.Tech(CSE,2013) from Lovely Professional University,Phagwara, Punjab. Interests are Artificial Intelligent System, Biometrics, Network Security and System Security.

Harjeet Kaur is the Assistant Professor in the Deaprtment of Computer Science and Engineering at Lovely Professional University. She has 14 year of teaching experience. Her areas of interest include Databases,Netwrk Security and Cyptography.

Scale Invariant Feature Transform Based Multimodal Biometric System with Face and Finger: A Review

Shubhangi Sapkal
Govt. College of Engg.
Aurangabad, India

Dr. R.R. Deshmukh
Dr. BAM University
Aurangabad, India

Abstract - Biometrics has long been known as a robust approach for person authentication. The face is one of the most acceptable biometrics because it is one of the most common methods of recognition that humans use in their visual interactions. In addition, the method of acquiring face images is nonintrusive. It is very challenging to develop face recognition techniques that can tolerate the effects of aging, facial expressions, and the variations in the pose of the face with respect to camera. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no single biometric is optimal. To reduce limitations of biometrics, multimodal biometrics can be used. This paper deals with a biometric authentication system by fusing face and finger images. Scale Invariant Feature Transform (SIFT) is used to extract invariant features from images.

Principal Component Analysis (PCA) and Fisher Linear Discriminant (FLD) are commonly used feature extraction methods for face recognition. In this paper, the focus is on perspective biometrics method based on facial and finger images using Scale Invariant Feature Transform. Image features generation transforms an image into a large collection of feature vectors, each of which is invariant to image translation, scaling, and rotation. It is useful due to its distinctiveness, which enables the correct match for keypoints between subjects. These features can be used to find distinctive objects in different images.

Keywords- SIFT, Biometric, Keypoints, Security, Person Identification, Scale invariant.

I. INTRODUCTION

In order to overcome the shortcomings of biometric system, fusion of two or more modalities of biometrics can be applied. Biometric fusion consolidates the output of multiple biometric classifiers to render a decision about the identity of an individual. Early research in this area dealt with decision level fusion. While only few papers have appeared in the area of feature level fusion and sensor level fusion, while score-level fusion has received considerable attention in the literature. Evidence in a multi-biometrics system can be integrated in several different levels: Sensor level, Feature level, match-score level, decision level. Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. It is used in environments that require high levels of accuracy, robust security, and solid customer service.

Multimodal biometric systems overcome some of the limitations associated with unimodal biometric systems such as noise in sensed data, intra-class variations, distinctiveness, non-universality, spoof attacks etc, by combining the data from different biometrics using an effective fusion rule, thus achieving higher accuracy and better performance. Fusion at the sensor level and feature level are expected to perform better than fusion at the other two levels, because there are more information about person identity[1],[2]. It has been observed that, a biometric system that integrates information at an earlier stage of processing is expected to provide more accurate results than the systems that integrate information at a later stage. Fusion at the sensor and feature level is expected to provide better recognition performances. But feature level fusion is difficult as feature vectors are not compatible and efficient fusion method is required.

In this paper, the method is proposed for combining face and fingerprint biometrics using SIFT and get score densities for these fused images. It has been proved that SIFT has very good performance in object recognition and other machine vision applications[3],[4], and is also used for face recognition[3]. Sovel *et. al.*, proposed a discriminative scale invariant feature transform (D-SIFT) for facial expression recognition [5] and Warren *et. al.* used it in medical imaging[6]. To ensure robustness, face-recognition algorithms have often worked in conjunction with fingerprint, iris, gait, and voice-recognition systems. This has led to the creation of a new research area: multimodal or

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

multibiometrics systems. A salient challenge in fusing biometrics algorithms or systems is to devise efficient and robust fusion methods[7]. Faisal *et. al.* showed that performance in face recognition system is improved in data level fusion than score level fusion[8].
Section 2 of this paper, deals with the related work in this area. Section 3 discusses about multibiometric system. Section 4 describes proposed method of feature extraction by SIFT. Sections 5 and 6 deals with image fusion and conclusion, respectively.

II. RELATED WORK

Author[9], apply SIFT descriptors to 2-D matrices for 3-D face recognition. Rattani[10], used feature level fusion of face and fingerprint. SIFT features are extracted for face and minutiae points for fingerprint. In [11], unsupervised discriminant projection (UDP) technique is used to identify a person with face and palm biometrics. Author[3], presented an application of the SIFT approach to the face recognition and proposed a new method based on SIFT and Support Vector Machine (SVM) for the face recognition problem. In[12], author worked on extraction of distinctive invariant image features that can be used to find the correspondence between different views of an object or a scene.
SIFT is used as an automatic computer assisted diagnostic system for renal cell carcinoma subtype classification[13]. Wang *et. al.*[14] presents the method for face based human verification using PCA. Score level fusion is done for face and voice in [15], [16]. Asha *et. al.*[17] proposed an authentication system with multi- biometrics to support various services in e-Learning where user authentication is necessary.

III. MULTIBIOMETRIC SYSTEM

Multibiometric system reduces some of the limitations observed in unimodal biometric systems. Biometric methods of human identification have gained much attention recently, mainly because they easily deal with most problems of traditional identification. Biometric technology—the automated recognition of individuals using biological and behavioral traits—is a natural identity management tool that offers high security and convenience than traditional methods of personal recognition. In addition to other applications biometrics is used in access control systems, where it recognize individuals already known to the system and allow them access to secured spaces. Several systems require authenticating a person's identity before giving access to resources. The key to multimodal biometrics is the fusion of various biometric modality data. In general, multimodal biometrics is based on the notion that the sets of data obtained from different modalities are complementary to each other. An appropriate combination of such data sets can be more useful than using the data from any single modality.

IV. SIFT FEATURE EXTRACTION

Feature vector detector seeks out points in an image that are structurally distinct, invariant to imaging conditions, and stable under geometric transformations. Lowe [18] presented a method for extracting distinctive invariant features from images that can be used to perform reliable matching between different views of an object or scene. SIFT can be used for feature extraction from face and fingerprint images. The features are invariant to image scaling and rotation, and partially invariant to change in illumination.
Following are the major stages of computation used to generate the set of image features[18],[19]:
i) Scale-space extrema detection: The first stage of computation searches over all scales
and image locations. It is implemented efficiently by using a difference-of-Gaussian function to identify potential interest points that are invariant to scale and orientation.
The scale space of an image is defined as a function, $L(x, y, \sigma)$ that is produced from the convolution of a variable-scale Gaussian, $G(x, y, \sigma)$ with an input image, $I(x, y)$:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y)$$

Where * is the convolution operation in x and y

$$G(x, y, \sigma) = \frac{1}{2\prod \sigma^2} e^{-(x^2+y^2)/2\sigma^2}$$

Difference of two nearby scales separated by a constant multiplicative factor k,

$$D(x, y, \sigma) = (G(x.y.k\sigma) - G(x, y, \sigma)) * I(x, y)$$

$$= L(x, y, k\sigma) - L(x, y, \sigma)$$

ii) Keypoint localization: At each candidate location, a detailed model is fit to determine location and scale. Keypoints are selected based on measures of their stability.

iii) Orientation assignment: One or more orientations are assigned to each keypoint location

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

based on local image gradient directions. All future operations are performed on image data that has been transformed relative to the assigned orientation, scale, and location for each feature, thereby providing invariance to these transformations.

For each image sample, $L(x, y)$, at this scale, the gradient magnitude, $m(x, y)$, and orientation, $\theta(x, y)$, is precomputed using pixel differences:

$$m(x, y) = \sqrt{(L(x+1, y) - L(x-1, y))^2 + (L(x, y+1) - L(x, y-1))^2}$$

$$\theta(x, y) = \tan^{-1}((L(x, y+1) - L(x, y-1)) / ((L(x+1, y) - L(x-1, y))$$

iv) Keypoint descriptor: The local image gradients are measured at the selected scale in the region around each keypoint. These are transformed into a representation that allows for significant levels of local shape distortion and change in illumination.

V. IMAGE FUSION

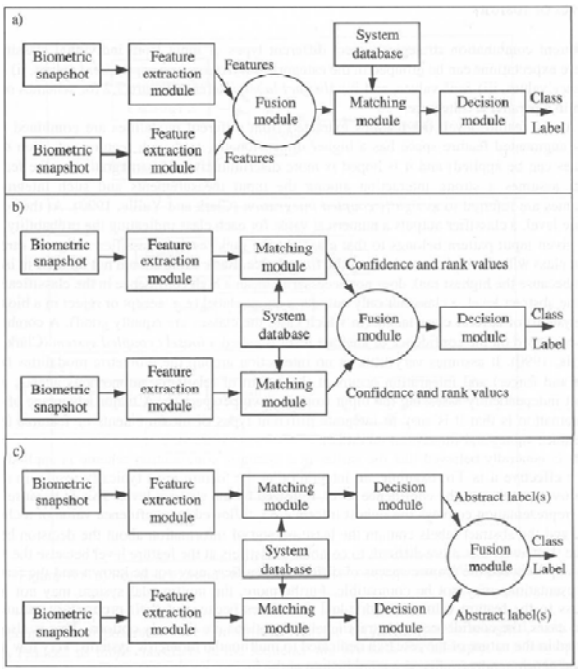


Figure1: Image fusion

The data presented by multiple levels can be integrated at various levels – Data level, Feature level, Score level and Decision level. Two new parameters, fusion factor (FF), and fusion symmetry (FS), will provide useful guidelines to select best fusion algorithm[20]. Feature level fusion is not accepted generally, as most commercial systems do not provide access to information at this level. It is also difficult to fuse data at feature level because of incompatibility of different feature spaces of biometrics traits. At decision level, limited information is available for fusion[2]. Decision level or score level fusion are commonly used levels of fusion.

VI. CONCLUSION

Now a days large scale multibiometric systems have been either proposed or deployed – US-VISIT, FBI database, India UID card etc. This shows that attention of researchers towards multibiometrics is necessary. Multibiometric systems can address the problems of non-universality and spoofing in addition to matching performance. We discussed the approach that can be used for multimodal biometric system. Major challenge in multimodal biometrics is of finding the optimal approach to combine different biometrics, and algorithms. This challenge is expected to continue for the coming years.

REFERENCES

1. Gunawan Sugiarta, Riyanto Bambang, Hendrawan, and Suhardi, “Feature Level Fusion of Speech and Face Image based Person Identification”, International Conference on Computer Engineering and Applications, 2010 IEEE, pp.221-225.

2. Anil K. Jain and Arun Ross, “Multibiometric Systems”, Communications of the ACM, January 2004, Vo. 47 No. 1, pp. 34-40.

3. Lichun Zhang, Junwei Chen, Yue Lu, and Patrick Wang, “Face Recognition Using Scale Invariant Feature Transform and Support Vector Machine”, International Conference for Young Computer Scientists, 2008 IEEE.

4. Qiu Tu, Yiping Xu, and Manli Zhou, “Robust Vehicle Tracking based on Scale Invariant Feature Transform”, IEEE International Conference on Information and Automation June 20 -23, 2008, Zhangjiajie, China.

5. H. Soyel and H. Demirel, “Facial expression recognition based on discriminative scale invariant feature transform”, Electronics Letters, March 2010, Vol. 46, No. 5.

6. Warren Cheung, Ghassan Hamarneh, “*N*-SIFT: *N*-Dimensional Scale Invariant Feature Transform for Matching Medical Images”, 2007 IEEE.

7. Rama Chellappa, Pawan Sinha, P. Jonathon Phillips, “Face recognition by computers and humans”, 2010 IEEE.

8. Faisal R. Al-Osaimi, Mohammed Bennamoun, and Ajmal Mian, “Spatially Optimized

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Data-Level Fusion of Texture and Shape for Face Recognition", IEEE Transactions on Image Processing, Vol. 21, No. 2, February 2012, pp. 859-572.

9. Tolga Inan and Ugur Halici, "3-D face recognition with local shape descriptors",IEEE transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012, pp. 577-587..

10. A. Rattani, D. R. Kisku, M. Bicego, and M. Tistarelli, "Feature Level Fusion of Face and Fingerprint Biometrics", 2007 IEEE.

11. Jian Yang, David Zhang, Jing-yu Yang, and Ben Niu, "Globally Maximizing, Locally Minimizing: Unsupervised Discriminant Projection with Applications to Face and Palm Biometrics", IEEE Transactions on pattern Analysis and Machine Intelligence, Vol. 29, No. 4, April 2007.

12. Gul-e-Saman, S. Asif M. Gilani, "Object Recognition by Modified Scale Invariant Feature Transform, 2008 IEEE.

13. S. Hussain Raza, Yachna Sharma, Qaiser Chaudry, Andrew N. Young, May D. Wang, "Automated Classification of Renal Cell Carcinoma Subtypes Using Scale Invariant Feature Transform", International Conference of the IEEE EMBS Minneapolis, Minnesota, USA, September 2-6, 2009IEEE.

14. Yongjin Wang, KN. Plataniotis, "Face based Biometric Authentication with Changeable privacy preservable templates", 2007 IEEE.

15. F. Alsaadea, A.M. Ariyaeeiniaa, A.S. Malegaonkara, M. Pawlewskib, S.G. Pillay, "Enhancement of multimodal biometric segregation using unconstrained cohort normalization", Pattern Recognition 2007, pp. 814-820.

16. Mingxing He, Shi-JinnHorng, PingzhiFan, Ray-ShineRun, Rong-JianChen, Jui-LinLai, Muhammad KhurramKhan, KevinOctaviusSentosa, "Performance evaluation of score level fusion in multimodal biometric systems", Pattern Recognition 2010, pp. 1789-1800.

17. S.Asha, Dr.C.Chellappan, "Authentication of E-Learners Using Multimodal Biometric Technology", 2008 IEEE.

18. David G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints", International Journal of Computer Vision, 2004.

19. Leidy P. Dorado-Munoz, Miguel Velez-Reyes, Amit Mukherjee and Badrinath Roysam, "A Vector SIFT detector for interest point detection in Hyperspectral imagery", IEEE transactions on Geoscience and Remote sensing, Vol. 50, No. 11, Nov. 2012, pp. 4521-4533.

20. Qiang Wang, Daren Yu, Yi Shen, "An overview of image fusion metrics", I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore, May 2009, pp. 1-6.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A Novel approach to provide 4 level High Security for the Mass of Cloud Data

R. Balasubramanian [#1]
Research Scholar, Comp.Sc.& Engineering,
Manonmanium Sundaranar University,
Tirunelveli, Tamilnadu, India.
Email: bala.rec@gmail.com

Dr.M.Aramuthan, [#2]
Department Of Comp.Sc & Engineering
Perunthalaivar Kamarajar Institute of Eng.& Technology
Karaikal, Pondicherry,India
Email: aranagai@yahoo.co.in

Abstract:

In the world of Information Technology cloud computing is one of the emerging technologies. Cloud computing provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. When this cloud is made available for the general customer on pay per use basis, it has some security issues that must be considered during its deployment. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. Hence the primarily aim is to highlight the major high security issues existing in current cloud computing environments. Keeping in mind of the security required, this paper introduces a four level high security approach in the mass of cloud data. This new approach will give high security for the customer as well as the cloud storage service providers.

Key Words: Cloud Storage Service; Authentication; User Level Security; Data Level Security; Shared Level Security; Maintenance Level Security; Cloud server ; Service Provider.

I. INTRODUCTION

Cloud computing is an upcoming and growing fast technology in the IT industry. Cloud computing provides a sharable platform, sharable software and pay and use Infrastructure. It also manages and schedules the resources under network, and having a big pool of network computing resources which provides services to the customer on demand. Basically the cloud is a network which provides dynamical resources as a service over internet based on the demand under payment with terms and conditions. There are three ways the cloud provide service to the world is PaaS[Platform as a service], IaaS[Infrastructure as a Service], SaaS [Software as a Service].

Cloud Computing can also be defined as the shifting of computing resources like processing power, network and storage resources from desktops and local servers to large data centers hosted by companies like Amazon, Google, Microsoft etc. There are many free online storage service is also available to the public like Apple iCloud, MS-SkyDrive, GoogleDrive, Amazon S3, BOX, DropBOX etc., but security is very low. The Cloud Storage Service [CSS] ability is to support the customer security needs effectively. In cloud storage service, clients upload their data together with authentication information to cloud storage server. Currently there are many security threats in cloud computing. The aim of this study is to provide a new approach for giving high security in cloud computing.

This paper introduces the 4 – levels of security as:

- One is the User Level Security [ULS], a secured Authentication and Authorization can be done. Here finding out how the customer will handle access to the cloud, including the verification of user credentials, determined level of access and determined place of access.
- The second one is Data Level Security [DLS], where security architecture of the system is designed by using AES cipher block chaining, which eliminates the fraud that occurs today with stolen data. There is no danger of any data sent within the system being intercepted, and replaced.
- Third one is Shared Level Security [SLS], where the data of one owner can share files to their known people by sharing key information.
- Finally Maintenance Level Security [MLS] is applied by giving a Proof of Retrievability Model [POR] and it depends on the customer offer system maintenance and upgrades.

Our work is structured as follows: in section 2 we describe our methodology of four level security model and we

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

present the experimental results in section 3. Then we present the conclusion in section 4.

II. RELATED WORK

Rahimli, Ailar [1] discussed in detail about the significant role of cloud provider and cloud user in providing the security in cloud.

Cloud computing RAS (Reliability, Availability, and Security) issues are summarized by Sabahi.F [2].In his paper he pointed out virtualization level of cloud computing security in detailed view.

Salesforce.com white paper [3] explains the terms security, privacy, and trust, and then explores the basic requirements for secure cloud computing. Subsequent sections of his paper provide a comprehensive introduction to the inherent security and privacy features of the Force.com enterprise cloud computing platform as well as platform features application providers can in turn use to build and secure their applications and customer data.

V.Krishnareddy, Dr. L.S.S.Reddy[4] described the Security Architecture of Cloud Computing. They tried to emphasize the main security issues existing in cloud computing environments. The security issues at various levels of cloud computing environment are identified in their paper and categorized based on cloud computing architecture. Their paper focuses on the usage of Cloud services and security issues to build these cross-domain Internet-connected collaborations.

The Multi-level user authentication system by using fuzzy based approach and log management method based on consumer behavior for applying IDS effectively to Cloud Computing system are proposed by Poorvadevi. R, Dr. K. Ramar [5]. The existing authentication systems are unable to provide the sufficient security and user Identification techniques. They proposed a scheme, trying to provide the Optimistic user signature identification through mining analysis and also using Fuzzy logic based user classification module provide the sufficient security for the cloud service access. Their scheme reduces the complexity involved in the key exchange process in cryptographic techniques. They tried to prove that proposed scheme will provide sufficient user classification and security with the help of strong mining tools and fuzzy computations.

The technical characteristics of cloud computing, analyses information security in cloud computing, security strategies and challenges that Cloud Service Providers (CSP) or vendors face during cloud engineering are discussed by Jijo S. Nair,Mukesh Kumar[6].

Kuyoro S. O., Ibikunle F. &Awodele O[7] explained Cloud Computing Security Issues and Challenges. Their paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

K.S.Suresh K.V.Prasad [8] describe about the different security algorithms, security issues and security attacks in cloud computing.

The very biggest problem associated with cloud computing is data privacy, security, anonymity and reliability etc. But the most important between them is security and how cloud provider assures it. Mandeep Kaur, Manish Mahajan [9] proposed a work plan to eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in cloud as per different perspective of cloud customers.

DES Algorithm in Cloud for Data Security is implemented by Neha Jain and Gurpreet Kaur [10]. Though many solutions have been proposed, many of them only consider one side of security. The main contribution of their paper is the new view of data security solution with encryption, which is important and can be used as reference for designing the complete security solution.

A new approach on Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds is given byMd Kausar Alam, Sharmila Banu K [11].In their paper they applied multi clouds concept using Shamir's Secret Sharing algorithm that is to reduce risk of data intrusion and loss of service availability for ensuring data.

By using AES algorithm an Enhancing Cloud Computing Security was developed by Abha Sachdev and Mohit Bhansali. Article [12] . In their paper they proposed a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data confidentiality and security.

Parsi Kalpana, et al [13] discussed the Data Security in Cloud Computing using RSA Algorithm. Even though the Cloud Computing is promising and efficient, there are many challenges for data security as there is no vicinity of the data for the Cloud user. To ensure the security of data, they proposed a method by implementing RSA algorithm.

B.Arun,S.K.Prashanth,[14] have presented a research paper on "Cloud Computing Security Using Secret Sharing Algorithm". The use of multi-cloud providers to maintain security has received less attention from the research community than the use of single clouds. This work aims to promote the use of multi-clouds to reduce security risks.

Bina Kotiyal,Priti Saxena, R.H.Goudar,Rashmi.M. Jogdand,[15] have presented a paper" A 5 Level Security Approach for Data Storage in cloud". In their paper they provide a new approach to the authentication process at various levels of cloud environment by replacing the concept of plain password storage with the hash password storage.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

To give high level security in cloud computing we propose four levels of security and are explained in detail in the subsequent sections.

III. PROPOSED PROBLEM STATEMENT

The usage of cloud is increase rapidly in all the organization. The providers should provide low cost and easy fast acceptance of the cloud. Also the Cloud providers should address privacy and security issues as a matter of high and urgent priority. Mainly the possibilities of the malicious insider in the cloud should be avoided. From the current research it is confirmed that the security in the single cum multi cloud has received less attention. To provide maximum complete security for the cloud this paper brings a novel approach gives security in four levels.

A. Proposed Security Model:

We propose a four level security model for cloud computing that provides us ULS, DLS, SLS and MLS in fig 1.

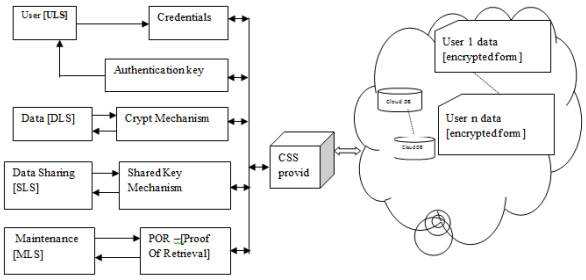


Figure.1 – Four Levels Securities in cloud

B. User Level Security [ULS]:

The first level security, in the current approach is when a common user request for cloud user the CSS looks for a high level authentication and provides authorization. When, user sends a request to cloud service provider it ask the user to fulfill a big list of credentials and gives a rank. If the rank reaches a threshold value then it generates a random authentication key to the user. The user now and then can enter into the cloud and utilize the minimum search level cloud data. Now the cloud user wants to go for further using of the cloud models SaaS, IaaS, PaaS, he is suppose to make the payment according to the level of usage and time. The three key cloud delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). In IaaS, the user can benefit from networking infrastructure facilities, data storage and computing services. Example: Consider the cloud space is 1GB for one year and he is supposes to make the payment of 8K to 10K to the service provider. In this paper it assumes that the user requests for an IaaS usage, the user converts into cloud user and gets authorized key from the cloud service provider after payment confirmation. Now the user can use the cloud space deploy and undeploy his data into his cloud space which named in the name of the user password connected with some secret key. Example the user password is rahumithra means the cloud space name is ***rahuXXX. Once the user try to open the cloud space, the CSS looks for authentication. The process is shown diagrammatically in fig 2.

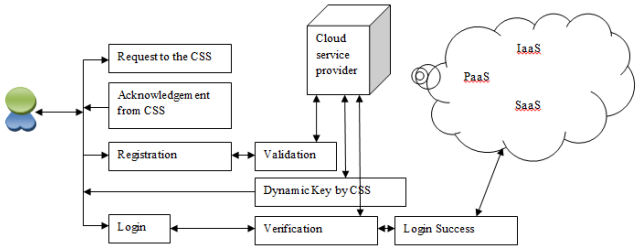


Figure.2: User Level Security

C. Data Level Security [DLS]:

After the user changed as a cloud user and the infrastructure that is owned and managed by users is in the private cloud. Data that is accessed and controlled by trusted users [registered user after authorization] is in a safe and secure private cloud, whereas the infrastructure that is managed and controlled by the cloud service provider is in a public cloud. The data may be unsafe and touched by untrusted users also. To avoid that, while uploading the user data it send to the crypt engine which encrypt the data into unreadable format, it protects the data stored in the cloud. The old methods used hash functions and the hash keys are stored in local memories. Again the local memory, hash keys are purely dynamic the key may get loss. Instead, in this paper the pair wise key generation and key distribution methods are used to give a dynamic key for encrypting the data and the key should be known only by the cloud user. While decrypting the data [and downloading] the user should pass the key with the POR information. The data can be viewed by the user in readable format. It is diagrammatically represented in fig 3.

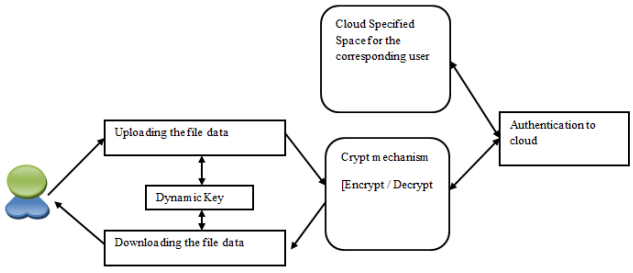


Fig 3 . Data Level Security

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

D. Shared Level Security [SLS]:

The data can be protected by using the single password given to many users by providing a security question with common answer and a dynamic key send to the owner and owner will pass it to the team people, and they can proceed. The detailed procedure of the shared level security is given in fig 4.

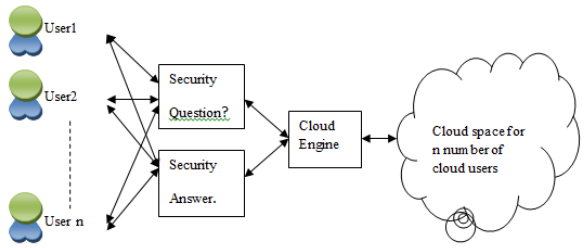


Figure.4 – Shared Level Security

E. Maintenance Level Security [MLS]:

Maintenance level security is provided to a lock system to all the data folders in the cloud. The cloud space is nothing but a folder which is created and assigned to the registered users in the cloud after made the payment. The space of the infrastructure is depends on the payment limit which is described in the problem statement. The folder name of each user is associated to the user information like password, username, dynamic key related etc. When user tries to accept the other users' folders gets fail also the data owner tries to accept his file with wrong password more than 3 times gets fail. So the data owner should remind his information for entering into the cloud is very particular and the login time by the data owner is limited. Example if the payment is over, and the amount paid is between 6k to 8k, he can use a space of 1GB under his name .For Example his name is Mr.Ram and the id is 001 from America, the folder name is amram001, Mr.Jam from Malaysia, id is 002 then his folder name is dmyjam002, where d indicates the destination. If anyone try to accept the others folder their id, name, destination all will be compared and access denied. It is diagrammatically represented in fig 5.

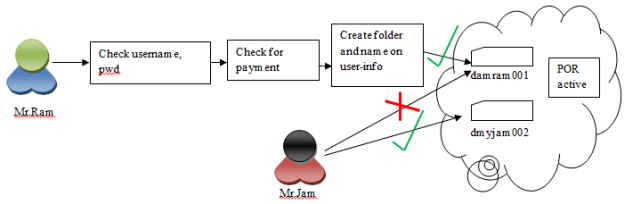


Figure.5 – Maintenance Level Security

F. Overall System model:

In this paper the overall system defines a new user enter into the cloud by registration. Once registration over the user become cloud user and gets a dynamic authentication key from the cloud server, used for further cloud activity initially [like searching, browsing]. If the user wants to use further IaaS, SaaS, PaaS, should make a payment according to the usage level and the time period going to use. The detailed structure is given in the following diagram fig 6.

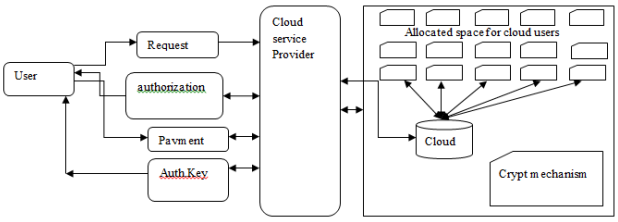


Figure-6: Overall System Model

IV. NOVEL APPROACH FOR CLOUD SECURITY

The pseudo code of the proposed Novel approach is given below for the developers to provide high security in their cloud computing.

- Let G be the cloud // private or public
- There are S, I and P ∃ SaaS, IaaS,PaaS in the cloud.
- u -> request -> G
- if { all credentials are valid} then
  - u -> U. where U = {u1, u2,….ui,….un} set of all
  - users in cloud.
  - u <- dynKEY; // u gets dynamic key value for login
- else
  - G rejects u.
- end
- u -> request -> cloud(PaaS,SaaS,IaaS);
- u -> makePay(uid, place, pwd, amount, DBsize);
- if (payment.Success = true)
- U <- checkCredentials(); // uid, place, amount, payment all entries
- createFolder(place,name,uid)
- Permission = true;
- else
- permission = false;
- end

SubProcedure 1

Public String **makePay** (uid, amount, fromNo, ToNo)

{

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

If ((Amount transferred from fromNo -> ToNo) == 0)

return payment.Success = true;

else

return payment.Success = false;

}

SubProcedure 2

Public String **checkCredentials()**

{

If (registeredusername == entryusername && registereduid == entryuid && registeredplace == entryplace)

makePay(uid, amount, accno1, accno2)

else

display “invalid data”

end

}

V. EXPERIMENTS AND RESULTS

The implementation of the proposed novel approach is done in visual studio 2010 software. The following figures are the real time screen shorts taken from the implemented software. The Figure-1, Figure-2 shows the Main and Registration page for the Existing/ New user. New user can enter by Registering into the cloud or by Login to the cloud. Once the User makes the registration, payment and request form, the CS generate and provide a dynamic key to the user for further precedence. So here after the user should take the key as the password for their cloud operations like upload and Download their data in the cloud.

Figure-1: Existing / NEW User can Enter

The Normal web users become the cloud user by registering themselves into the cloud by filling the credential forms given by the CSP. After Registration they can login to the cloud and utilize the basic browsing and searching operations.

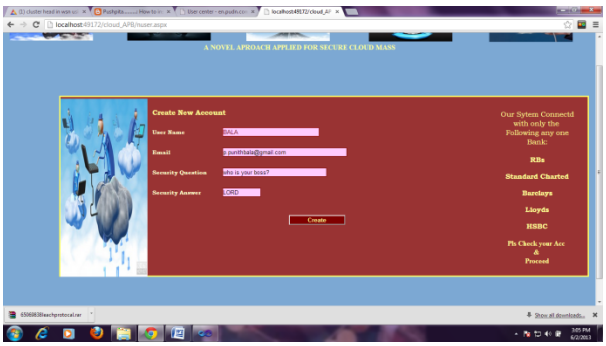


Figure-2: New User can Enter by Registration

Since, the user becomes a cloud user they also utilize the IaaS, SaaS, PaaS of the cloud by registering to the second level with the payment according to the usage level and the period of using the cloud resources, it may be any resource.

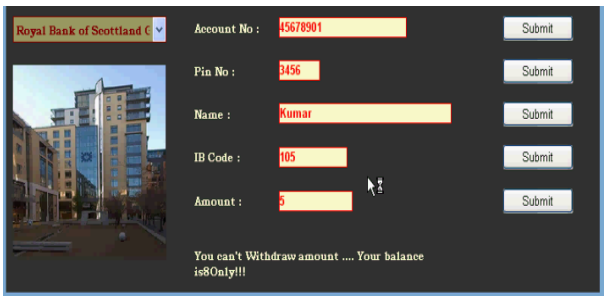


Figure-3: Authorization by CS [ULS]

Once the user become the cloud user, for further resource utilization they should make the payment.

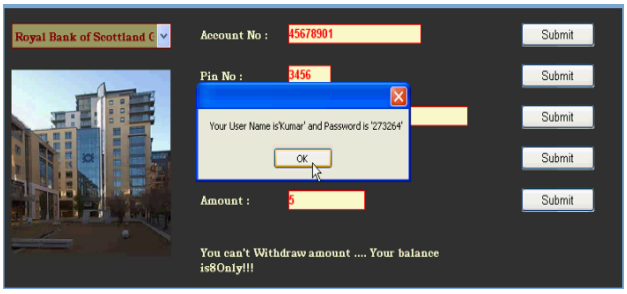


Figure-4: Pin Number given after successful payment.

Once the payment made successfully, the CSP provide a dynamic pin number as password

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Figure-5: POR is checking the user location and name of the user while uploading. [MLS]

After payment the user can upload their files into the Infrastructure named in their names with related passwords.

Figure-6: POR restricts the user while folder belongs to the other user [MLS].

If the user tries to open other user folder then the POR compares the user login info with the folder ID and denials.

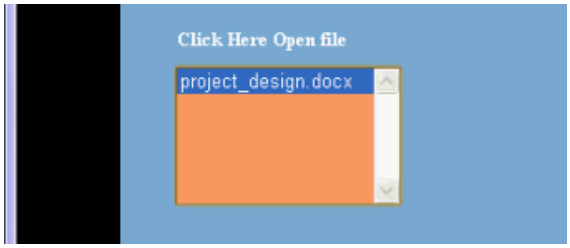


Figure-7: POR permits and opens the folder for Right user.

After the validation the POR permits the user to the folder and shows the files to the user.

In the complete implementation nearly 50 user become cloud user and nearly 50 clouds space is allocated. In that anomaly there are 12 users tried to open the other user's data folder. Out of 100 users there were 16 users tried to open other's data. They verified by the POR and it recorded their IP. Once if a user tries more than three times their IP address will get blocked and will get a reject message from the POR of the cloud. Figure-3,4 shows the distribution of Key to the community or data owner's Friends, then SLS will ask some frequent questions and make them to access the folder and files. The figure-7 shows the original file uploaded and downloaded by the Security mechanism in DLS.

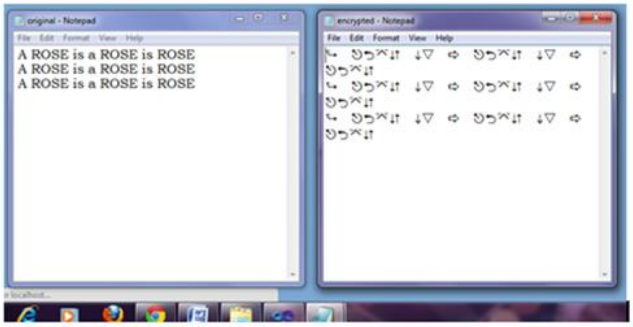
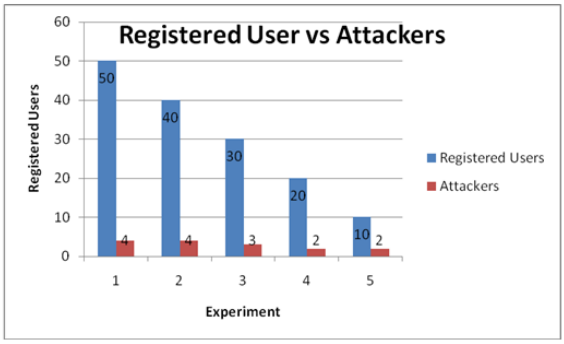


Figure-8: Original File & Encrypted File [DLS]

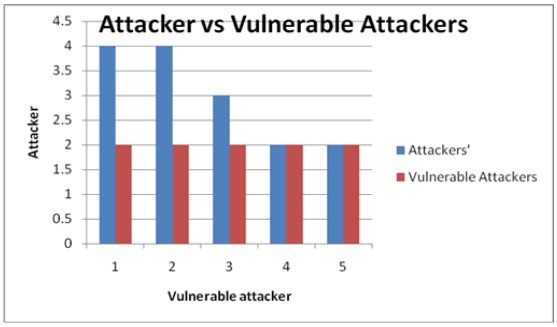
The Figure-8 shows the functionality if the DLS in the Cloud, where the first window shows the original file having the readable content is normal English, and the Second window shows the encrypted file having unreadable format. Even though we are applying security in UL, ML, SL, we also provide security in Data Level also. After attack, the attacker can't use the content of the file. From the implementation, there are two graphical output is analyzed. The complete optimized output of the cloud security is given in the form of Graph for Registered user vs Attacker. Attacker vs IP-address address blocked. Graph-1 shows the Number of registered Users vs attackers.



Graph -1: Registered User Vs Attackers

In our proposed approach we are detecting and avoiding the attackers, and if they cross their limit then we are eliminating from the cloud. It shows in the Graph-2.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500



Graph-2: Attackers Become Vulnerable Attackers

VI. CONCLUSION

There were many methodologies are available like privacy preserving, source anonymity, location preserving etc. even though till research is going on in security on cloud storage; the Secret methods are computationally inexpensive when compared with the traditional encryption techniques. In this paper the novel approach gives high security in all the levels and Data Leakage is Avoided 99%. Even the Data leaked the information on the data wont leaked. Also in the proposed system we are applying level by level security, where no one can escape from all the levels because all the level securities are inter related and connected by the dynamic authentication by the CS. Once dynamic validation is done the security value will get increasing, this paper also says the dynamic validation is done by ULS, DLS, SLS and MLS, in all the levels the CS is comparing the user credentials with IP address, dynamic key. So only the performance of this novel approach is high than other approaches and it is giving security nearly 99%. The one percentage the trusted Shared level security may become attackers.

Future Enhancement:

This proposed novel approach is providing high security and it is taking much time for validation and dynamic authentication. In future it can be enhanced into time effective also, because the times affect the cost.

REFERENCE:

[1] Rahimli, Ailar,"The role of the cloud provider to providing security incloud computing"International Journal of Research Studies in Computing,10 March 2013,

[2] Sabahi.F,"Virtualization-level security in cloud computing"Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on May 2011, pp:250-254

[3] Sales force .com white paper, www.salesforce.com/assets/pdf/misc/WP-Forcedotcom.security/pdf

[4] V.KrishnaReddy., Dr. L.S.S.Reddy,"Security Architecture of Cloud Computing", Vol.3 No. 9 September 2011,pp7149 –7155

[5] Poorvadevi. R, Dr. K. Ramar," An Efficient Implementation Of Validating The Client Level Security Factors For The Cloud Applications", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April – 2013,pp

[6] Jijo S. Nair, Mukesh Kumar," Policy for Security issues in Cloud Computing", International Journal of ComputationalEngineering Research (IJCER),pp 74 – 77

[7] Kuyoro S. O., Ibikunle F. &Awodele O. ,"Cloud Computing Security Issues and Challenges," International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011pp 247 -255

[8] K.S.Suresh K.V.Prasad,"Security Issues and Security Algorithms in Cloud Computing" Volume 2, Issue 10, October 2012 *IJARCSSE* – pp 110-114

[9] Mandeep Kaur,Manish Mahajan,"Using encryption Algorithms to enhance the Data Security in Cloud Computing**"** International Journal of Communication and Computer Technologies, Volume 01 – No.12, Issue: 03 January 2013,pp 56-59

[10] Neha Jain,Gurpreet Kaur ,"Implementing DES Algorithm in Cloud for Data Security"VSRD-IJCSIT, Vol. 2 (4), 2012, pp 316-321

[11] Md Kausar Alam, Sharmila Banu K,"An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds "International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013

[12] Abha Sachdev and Mohit Bhansali,"Enhancing Cloud Computing Security using AES Algorithm", International Journal of Computer Applications 67(9), April 2013.): pp19-23 Published by Foundation of Computer Science, New York, USA.

[13] Parsi Kalpana ,et al," Data Security in Cloud Computing using RSA lgorithm",International Journal of Research in Computer and Communication technology, IJRCCT, Vol 1, Issue 4, September 2012

[14] B.Arun,S.K.Prashanth,"Cloud Computing Security Using SecretSharing Algorithm",Indian Journal of research, Volume : 2 , Issue : 3 , March 2013, pp 93-94

[15] Bina Kotiyal,Priti Saxena, R.H.Goudar,Rashmi.M. Jogdand," A 5 Level Security Approach for Data Storage in cloud", IJCA,Vol. 54-No11, September 2012 pp 29-34

AUTHORS PROFILE

[#1] I, Balasubramanian, studied Bachelor and Master of Engineering in Computer Science and Engineering at National Institute of Technology, Trichy, TamilNadu, India (formerly Regional Engineering College, Trichy). I have 5 years of teaching experience and about 9 years of experience in IT industry.

[#2] I, Aramudhan, studied Bachelor and Master of Engineering in Computer Science and Engineering at National Institute of Technology, Trichy, TamilNadu, India (formerly Regional Engineering College, Trichy). I did my Ph.D in Computer Science and Engineering at Indian Institute of Technology, Chennai, TamilNadu, India. I have 15 years of teaching experience.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Practical Routing Strategy in Delay-Tolerant Networks: A Survey

Lalitesh Kumar Choudhary
CSE, UIT, RGPV
Bhopal, India
lalitesh.choudhary@yahoo.com

Manish Kumar Ahirwar
CSE, UIT, RGPV
Bhopal, India
ahirwarmanish@gmail.com

Uday Chaurasiya
CSE, UIT, RGPV
Bhopal, India
uday_chourasiya@rediffmail.com

***Abstract*- A delay tolerant network is a special type of emerging network that experience frequent and intermittent connectivity or delays during communication. Also the delay tolerant network is a partition based network in which at any given time, the path between source and destination does not exist by which we may conclude that two nodes may never exist in a one connected portion of the network. As compared to conventional network the distinguishing feature can be summarized by two points i.e. Delay (Since there is no fixed connectivity and hence messages take time until they reach the destination) and resource constraints (Since all the nodes carry some limited buffer, it has to drop older messages if the buffer gets full in order to accommodate new messages). In this paper we have given emphasis on the various DTN routing approaches along with its pros and cons.**

Keywords- Delay tolerant network; Knowledge Oracle; Custody Transfer

I. INTRODUCTION

The name delay tolerant network is given by kevin fall of intel research group [3] , in which they proposed a network architecture as well as an application interface for asynchronous message forwarding in a partition based network which suffer from continuous topology change and extremely long delay (may be in days).In such network finding the destination node and the way to route the packet to the intended destination to insure the robust communication is a major challenge . Delay tolerant network is a one type of infrastructure less wireless network in which most probably there does not exist a complete path between source and destination. The DTN works in a stressful environment [4] in which link

Disruption may result in excessive delays in message transmission during communication. The node in the delay tolerant network has the added constraint of finite buffers and no end to end path may ever exist .The above situation leads the problem [1] like High latency &low data rate, end to end node Disconnection Problem, Long message queuing Times, as well as Limited resources in terms of limited memory and processing capability.

The concept of DTN makes the use of store carry and forward mechanism in which first of all, the message to be sent to any node has to be stored or buffered in the form of bundle (basic unit). Then it is carried until it finds some interesting node (may be on the basis of some utility values).And as a last step forward the particular message to that node. This process continues until the message is delivered to the destination or is dropped due to network congestion or on the basis of Time to live (TTL) values. During the message transmission the reliability is achieved in DTN by making use of custody transfer mechanism. The concept of custody transfer can be defined as the data transfer mechanism, in which the responsibility of data segment (bundle or bundle fragment), migrates with the data as it progresses across a series of network hops for the purpose of reliable delivery on a hop-by-hop basis as compared to an end-to-end which is impractical over intermittently connected nodes.

The routing problem or in more clear term message forwarding strategy in delay tolerant network has been focused by the researchers in the last decades and they have used various parameters to classify the existing routing approaches. In this work we have tried to list all the routing approaches along with its pros and cons .

The rest of the paper has been organized in following ways. In section 2 we have listed the application domain, making use of DTN concept. In Section 3, we have outlined the alarming characteristics of delay tolerant network. Section 4 includes some DTN routing issues as well as performance metrics suited for challenged network. Classifications of routing strategies along various dimensions have been summarized in Section 5. Finally, some concluding remarks have been underlined in Section 6.

II. APPLICATION DOMAIN MAKING USE OF DTN

A various application area that makes the use of DTN concepts may include military applications, outer-space communication, wildlife tracking, underwater

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

monitoring, social networks, battlefields, developing region communication, vehicular ad hoc networks, and packet switched networks.

A. Interplanetary communication [27]

It is the extreme cases in which Delay tolerant network can be used. The large distances separating terrestrial objects restrict the conventional method to exchange data in between them or with base-stations on earth .The DTN application of interplanetary network overcomes the traditional limitation of TCP. Now the scientist from the base station on earth can control the operation of a robot working on Mars.

B. Military Applications

The DTN can be used for military applications by allowing the retrieval of critical information in mobile battlefield scenarios using only intermittently connected network. Military services can make good use of DTN architecture as the military camps may be located in very rough and difficult terrestrial area where4 it is not possible to establish a standard communication medium. In such a situation DTN seems much suitable to transmit and receive data.

C. Wildlife Tracking [25]

In the zebra net project, zebras are equipped with sensor neckband and these sensors are used to track animal movement and collect information related to zebras behavior. Through the zebra net project, zebra's mobility, migrations and interspecies interactions are going to be analyzed.

D. Connectivity in Underdeveloped Regions [26]

The aim of DakNet project is to Provide connectivity to remote villages with limited infrastructure installed in booths in order to provide basic services like E-mail, online banking facilities, awareness towards government norms. Connection enabled vehicle that passes through villages are used to provide communication facilities in between villages and the nearest city.

E. Inter-Vehicular and Vehicle-Infrastructure Connectivity

Now a day, vehicular network has gain the major attention of researchers in order to enhance the traffic safety and reduce the probability of a vehicle collision. Location dependent information may be used to predict the traffic congestion, available parking lots, ongoing road jamming problems etc.

F. Social Awareness and Pocket-Switched-based Networking

Delay tolerant networking can be used in this context by Making use of communication on the fly concept means the handheld communicating device may silently interact when they are in communication range of one another and notify the users through beep sound or popup messages.

G. Data collection in sensor network [28]:

Data mule is a one type of data collector which can be used to collect the data sensed by the no. of nodes sparsely deployed in an area. Data mule is a one type of mobile relay node used for the purpose of carrying data from energy constraints static sensor node to an infra - structured access point.

III. CHARACTERISTICS OF DELAY TOLERANT NETWORK

A. High latency &low data rate

As DTN are made of sparsely connected node that may never meet to each other which leads to high latency [1] as well as the low data transmission rate(up to 10kbps under water). Data rates may be largely asymmetric for example participating devices may have small uplink and high downlink.

B. Disconnection Problem

In the delay tolerant network scenario, end to end path does not exist; the node disconnection problem is much common as compared to conventional network. Here the nodes are highly mobile and some communicating devices may have limited processing capability (in the case of sensor network).

C. Long queuing Times

As the delay tolerant network makes the use of store carry forward mechanism in which a message may be needed to store for a long time in a buffer of a node before forwarding it. Also the queuing delay may vary depending upon the node meeting probability; means the queuing delay may be extremely large in worst case.

D. Interoperability Consideration

Delay tolerant network tends to be comparatively simple and local in scope. The DTN may use application specific framing format, limited node addressing and framing capabilities etc.

E. Limited resources

Resource constraints such as limited buffer capacity, processing capability, battery exhaustion of a node as well as an end to end delay due to the unexpected environment in between sender and receiver limits the availability or survivability of a node.

IV. ROUTING ISSUES FOR DELAY TOLERANT NETWORK

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Delay Tolerant Network routing protocol have been widely discussed in the last few years. The routing strategy for Delay tolerant network is based upon a problem of deciding a circumstance under which a message holding nodes forward or hand over its message copy to another node. To face the intermittent connectivity [2] we need to deploy a store carry and forward mechanism. In challenged scenario, next hop may not be immediately available, thus the bundle carrying node need to buffer the data until gets an opportunity to forward it. Also the DTN operation proceeds roughly in the following stages [14].

A. Neighbor Discovery: The node must discover one another before a transfer opportunity can establish; also nodes do not know when the next opportunity may exist.

B. Metadata transfer: information about buffer management and routing decisions are exchanged [5] between nodes after encountering each other.

C. Data Transfer: After above stages the data transfer may begin. Here the amount of data a node can transfer is limited and a node may go out of the communication range before completion of the data transmission. One way to deal with this situation is to fragment the data packet before transmitting it, known as proactive fragmentation or fragments the data into packets when the data has not been completely transmitted, known as reactive fragmentation.

D. Storage management: As packets are received in between neighboring nodes, each node must manage its finite size local buffer by selecting particular drop order of packets that has to be discarded in order to free up the buffer spaces for incoming bundles. To drop the packet it makes the use of certain indexes such as the received timing of the packet, remaining time of the messages, distance to the destination etc.

The various metrics [6] that can be defined in order to evaluate the performance of DTN routing protocol are:

A. Delivery ratio: It is the most important network performance metrics. As a DTN work in a challenging environment where the message is generally lost or dropped before reaching to the actual destination. This metric can be defined as the ratio of generated message to the correctly delivered message within a given time period. It should be the responsibility of the good routing protocol to enhance the packet delivery ratio.

B. Latency: It is the second most important network performance metrics. It is the indicator of end to end delay means it measures the time between when the message is generated at the source and when it is received at the destination. Thus we need to minimize the end to end delay.

C. Transmissions: This metric is used to measure the requirement of computational resources. For example in flooding or replication based routing scheme multiple copies of message are distributed, thus consumes more resources as compared to forwarding based routing scheme. As each participating component has limited resources, Thus the routing needs to use these resources (energy, bandwidth, buffer) in an intelligent manner.

By considering all the aspects of DTN we can specify few design goals for delay tolerant network routing protocol such as

A. Self Configuration: The routing protocol must be self configuring in the nature. As delay tolerant network suffers from intermittent connectivity, lack of fixed topology or battery exhaustion of a node may lead to the failure of some network component.

B. Performance Acceptablity: As in above paragraph we have seen that the DTN approaches are going to be used in many application domains. Thus our choosed routing protocol should provide acceptable performance over a wide variety of connectivity patterns means the protocol must be a good choice for most DTN scenarios.

C. Resource Constraint: Resource constraints are of major concern for DTN in the sense every node consists of limited buffering capacity, processing capability etc. thus the routing protocol must make efficient use of buffer and network resources.

D. Scaling Capability: And at last but not least the routing protocol must be capable of scaling with the demand.

V. VARIOUS ROUTING STRATEGY FOR DELAY TOLERANT NETWORK

The "*Routing*" in DTNs has been a very widely addressed matter that almost distinguished itself as an independent research area where a vast and rapidly increasing amount of works continue to appear. Routing consists of a sequence of independent, local forwarding decisions, based on current connectivity information and predictions of future connectivity information [5]. During which Data delivery only happens when two nodes are in contact in a DTN. Knowledge about contact schedules becomes important for routing in opportunistic network scenario [2]. The routing strategy for Delay tolerant network[4] is based upon a problem of deciding a circumstance under which a message holding nodes forward or hand over its message copy to another node. To face the intermittent connectivity. We need to deploy a store carry and forward mechanism. In challenged scenario, next hop may not be immediately available, thus the bundle carrying node need to buffer the data until gets an opportunity to forward it.

T. Spyropoulos et.al. in 2004 proposes two types of routing scheme that was single-copy routing scheme

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[12] and multi-copy routing scheme [29]. A single copy routing scheme uses single custody for each message throughout the network. A single custody implies that a single copy of the message exists in a particular time. A current message holding node forward a copy to the appropriate next node until the message reaches its destination. The example of single copy routing scheme[9] includes *randomized routing algorithm* in which the message is handed over to the encountered node with probability P , *utility based routing algorithm* defines a utility function which is maintained by each node for every other node for indicating the usefulness of message delivery as well as a *hybrid routing algorithm* termed as seek and focus routing algorithm which makes the use of both of the above algorithm i.e. randomized as well as utility based routing algorithm. On the other hand, multiple-copy routing schemes may be defined as a scheme in which multiple copies of message are spread throughout the network for the purpose of increasing efficiency as well as robustness. Further the multi copy routing scheme may be categorized into two groups based on the restrictions imposed on the no. of copies that is extremely flooding and controlled flooding [the example of multi copy routing scheme includes probabilistic routing, epidemic routing etc .The scenario of multi copy scheme may use flooding-based approach or restricted flooding based approach for example “Spray and Wait” Routing algorithm .first of all this routing algorithm spreads sufficient no. of message copies under the guarantee that at least one of them will reach the destination in a manner similar to epidemic routing. After that it stops and wait until each node carrying a copy perform direct transmission.

Z. Zhang, in [8], exposed a wide survey of the unicast routing schemes that have been published up until May 2006 including:

Deterministic schemes in which future network’s state/topology are predictable, hence allowing message forwarding to be scheduled ahead of time. The space time, tree-based, and modified shortest path are examples of deterministic routing schemes And Stochastic schemes where the future network’s state/topology is completely unknown and hence no pre-scheduling of transmissions can be done. The routing schemes that falls under these categories include Epidemic and randomized flooding, history-based, model-based, and coding based scheme.

Further the DTN routing task can be classified among three dimensions:

A. On the basis of the no. of message copy replicated throughout the network [3,5]

The DTN routing scheme may be classified into three broad categories that are flooding , replication and forwarding routing scheme. In flooding routing scheme[7] multiple copies of message are spread throughout the network for the purpose to increase the packet delivery ratio. Also a routing protocol of flooding families tries to reduce the packet delivery delay. In replication based routing scheme, the no. of messages spread throughout the network is restricted. Here the quota of the message (for replication) is decided based upon certain quota allocation function. This function may be static or dynamic. For example spray and wait routing protocol makes the static quota allocation function i.e. binary values whereas the dynamic quota based routing protocol [23] uses queuing or traffic demand oracle to decide the message replication quota. The forwarding routing scheme uses single custody for each message throughout the network. A single custody implies that a single copy of the message exists in a particular time. A current message holding node forward a copy to appropriate next node until the message reaches its destination. Some example of routing protocol that belong to forwarding families are fair route routing, simbet routing etc.

B. On the basis of knowledge oracle used

The DTN routing protocol may compute the optimal route based upon many input variables, complete knowledge of which may easily facilitate the way to compute efficient relaying routes in between two participating nodes. There exists a trade off between performance of routing protocols as well as a knowledge oracle used to find the best next hop node that may act as a custodian of the received bundle. A node may not use any of the knowledge oracle at all, for example in the case of epidemic routing protocol none of the knowledge oracle is used and it floods the packet blindly throughout the network to minimize the communication delay .On the other hand, we can see that a node may use partial knowledge regarding the network situation such as contact history of a node, load of the network , node movements etc. to enhance the network performance. Sushant Jain et.al [12] has classified these knowledge oracle into four categories that is contact summery oracle which provide average waiting time until the next contact for an edge, contact oracle which specifies contact between two nodes at any point of time, queuing oracle which makes the use of knowledge regarding buffer occupancy of a node and at last traffic demand oracle which can answer any question regarding present or future traffic demands and inject message according to the network traffic.

C. On the basis of decision type used

As Delay tolerant network suffers from intermittent connectivity where the nodes are sparsely distributed. The source node may use the source routing to determine the complete path of a message and encode this information some how in the messages. Thus the route is determined once and does not change during the traversal of the message throughout out the network. ON the other hand in per hop routing the next

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

hop of a message is determined at each intermediate hop. Here the message uses the local information regarding available contacts and queuing status of each node. The per hop routing [12] may enhance the network performance but it may lead to loops when nodes have different topological views.

TABLE I : SUMMARY OF EXISTING DTN ROUTING PROTOCOL WITH PROS AND CONS

Routing protocol	**Oracle type**	**Replication strategy**	**Decision type**	**Pros**	**Cons**
Epidemic [10]	None	Flooding	None	High packet delivery ratio	High resource consumption
Minimum expected delay[12]	Contacts Summary	Forwarding	Source Node	Minimize average waiting time,	No mechanism to deal with congestion
Prophet[11]	Contact Summery	Flooding	Per hop	Lower communication overhead	High network congestion
Spray and Wait [13]	None	Replication	Per hop	Low latency	Static quota allocation function
MaxProp [14]	Queuing	Flooding	Per hop	Better use of buffer and transmission opportunity	Network congestion problem
Spray and Focus [15]	Contact Summery	Replication/Forwarding	Per hop	High delivery ratio	Static quota allocation function
Distance Aware Epidemic Routing (DAER) [16]	Queuing	Flooding/Forwarding	Per hop	Better packet delivery ratio	High amount of knowledge oracle used
SimBet [17]	Contact	Forwarding	Per hop	Good packet delivery ratio,	40% more delay compared to epidemic
Delegation Forwarding [18]	Contact	Flooding	Per hop	Reduces relay cost	Dependent on past contact history
Vector Routing [19]	Traffic Demand	Flooding	Per hop	Good packet delivery ratio	Network congestion problem
Encounter–Based Routing [20]	Contact	Replication	Per hop	Minimize delivery ratio, minimize overhead and delay	Only Suitable for network having small no. of hop
Fair Routing[21]	Traffic Demand	Forwarding	Per hop	Fair load distribution	Low packet delivery ratio
RAPID [22]	Traffic Demand	Flooding	Per hop	Better utilization of resources	Suited for small network load
Dynamic congestion control based routing [24]	Queuing/Traffic Demand	Dynamic quota based replication	Per hop	Better congestion control	High amount of knowledge oracle used

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. CONCLUSION

DTN approaches are suitable for challenging environment where end to end communications are subject to delay and disruption. In this work we have focused on various stages of DTN operation as well as the performance metrics that needs to take under consideration at the time of designing the routing protocol. We have underlined some trade-off that has to be considered during a routing protocol design. First when we try to maximize the packet delivery ratio we need to shift silently from flooding based approach to forwarding approach in order to reduce the network congestion because of limited buffer availability or due to the access discarding of the packet. Secondly Compromise regarding the amount of information collected to guide the packets to their destinations is also a one type of tradeoff where a node needs to collect the utility information of the neighboring node in order to forward the packet. Also we have tried to categorize the families of DTN routing protocols among various dimensions in a tabular form.

REFERENCES

[1] K. Fall, “A Delay-Tolerant Network Architecture for Challenged Internets,” in Proc. ACM SIGCOMM Conf., pp. 27-34, Aug. 2003.

[2] J. Shen, S. Moh, and I. Chung, "Routing Protocols in Delay Tolerant Networks: A Comparative Survey," in Proc. Intl. Conf. Circuits/Systems,Computers and Communications, pp. 1577-1580, Jul. 2008.

[3] A. McMahon and S. Farrell, "Delay- and Disruption-Tolerant Networking," IEEE Internet Computing, vol. 13, no. 6, pp. 82-87, Nov.2009.

[4] Delay-Tolerant Networking Research Group (DTNRG),http://www.dtnrg.org

[5] S. C. Lo, M. H. Chiang, J. H. Liou, and J. S. Gao, “Routing and Buffering Strategies in Delay-Tolerant Networks: Survey and Evaluation,” in Proc. IEEE ICPP Workshop, Sept. 2011.

[6] E. P. C. Jones, L. Li, and P. A. S. Ward, "Practical Routing in Delay-Tolerant Networks," IEEE Trans. Mobile Computing, vol. 6, no. 8, pp.943-959, Aug. 2007.

[7] R. J. D'Souza and J. Jose, "Routing Approaches in Delay Tolerant Networks: A Survey," Intl. Journal of Computer Applications, vol. 1, no.17, pp. 8-14, 2010.

[8] Z Zhang" Routing In Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overviews and Challenges," in Proc. IEEE communication survey&tutorial,1st quarter 2006

[9]. T. Spyropoulos, K. Psounis, and C.S. Raghavendra, "Single-Copy Routing in Intermittently Connected Mobile Networks," in Proc. IEEE Intl. Conf. Sensor and Ad Hoc Communications and Networks, pp. 235-244, Oct. 2004.

[10] A. Vahdat and D. Becker, "Epidemic Routing for Partially-Connected Ad Hoc Networks," Duke University, Technical Report CS-200006, Apr. 2000.

[11] A. Lindgren, A. Doria, and O. Scheln. "Probabilistic Routing in Intermittently Connected Networks," LNCS, Springer, vol. 3126, pp. 239-254, 2004.

[12] S. Jain, K. Fall, and R. Patra, "Routing in a Delay Tolerant Network," in Proc. ACM SIGCOMM zonf., pp. 145-158, Aug. 2004.

[13] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and Wait:An Efficient Routing Scheme for Intermittently Connected Mobile Networks," in Proc. ACM SIGCOMM Workshop, pp. 252-259, Aug.2005.

[14] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "MaxProp:Routing for Vehicle-Based Disruption-Tolerant Networks," in Proc.IEEE INFOCOM Conf., pp. 1-11, Apr. 2006.

[15] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and Focus: Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility," in Proc. IEEE Pervasive Computing and Communications Workshops, pp. 79-85, Mar. 2007.

[16] H. Y. Huang, P. E. Luo, M. Li, D. Li, X. Li, W. Shu, and M. Y. Wu,"Performance Evaluation of SUVnet With Real-Time Traffic Data,”IEEE Trans. Vehicular Technology, vol. 56, no. 6, pp. 3381-3396, Nov.2007.

[17] E. M. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," in Proc. ACM MobiHoc Conf., pp. 32-40, Sept. 2007.

[18] V. Erramilli, M. Crovella, A. Chaintreau, and C. Diot, "Delegation Forwarding," in Proc. ACM MobiHoc Conf., pp. 251-260, May 2008.

[19] H. Kang and D. Kim, "Vector Routing for Delay Tolerant Networks," in Proc. IEEE VTC Conf., pp. 1-5, Sept. 2008.

[20] S. C. Nelson, M. Bakht, and R. Kravets, "Encounter-Based Routing in DTNs," in Proc. IEEE INFOCOM Conf., pp. 846-854, Apr. 2009.

[21] J. M. Pujol, A. L.Toledo, and P. Rodriguez, "Fair Routing in Delay Tolerant Networks," in Proc. IEEE INFOCOM Conf., pp. 837-845, Apr.2009.

[22] A. Balasubramanian, B. N. Levine, and A. Venkataramani, "Replication Routing in DTNs: A Resource Allocation Approach," IEEE/ACM Trans. Networking, vol. 18, no. 2, pp. 596-609, Apr. 2010.

[23] Shou-Chih Lo and Wei-Rong Liou,” Dynamic Quota-Based Routing in Delay-Tolerant Networks” in ieee 2012.

[24] Shou Chih Lo andChuan-Lung Lu,” A Dynamic Congestion Control Based Routing for Delay-Tolerant Networks” in ieee,FSKD 2012.

[25] The ZebraNet Wildlife Tracker, http://www.princeton.edu/~mrm/zebranet.html

[26] A. Pentland, R. Fletcher, and A. Hasson, "DakNet: Rethinking Connectivity in Developing Nations," Computer, vol. 37, no. 1, pp. 78-83, Jan. 2004.

[27] IPN Special Interest Group (IPNSIG), http://www.ipnsig.org/

[28] R. Shah et al., “Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks,” IEEE SNPA Wksp., May 2003.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Design and Implementation of Multi Factor Mechanism for Secure Authentication System

Khalid Waleed Hussein [#1], Dr. Nor Fazlida Mohd. Sani [*2], Professor Dr. Ramlan Mahmod [#3]

Dr. Mohd. Taufik Abdullah [#4]

Faculty Computer Science & IT, University Putra Malaysia (UPM)

Kuala Lumpur, Malaysia

Khaled_it77@yahoo.com

fazlida@fsktm.upm.edu.my

ramlan@fsktm.upm.edu.my

mtaufik@fsktm.upm.edu.my

***Abstract*: A secure network depends in part on user authentication and regrettably the authentication systems currently in use are not completely safe. However, the user is not the only party that needs to be authenticated to ensure the security of transactions on the Internet. Existing OTP mechanism cannot guarantee reuse of user's account by an adversary, re-use stolen user's device which is used in the process of authentication, and non-repudiation.**

This paper proposed mechanism of multi factor for secure electronic authentication. It intends to authenticate both of user and mobile device and guarantee non-repudiation, integrity of OTP from obtaining it by an adversary. The proposal can guarantee the user's credentials by ensuring the user's authenticity of identity and checking that the mobile device is in the right hands before sending the OTP to the user. This would require each user having a unique phone number and a unique mobile device (unique International Mobile Equipment Identity (IMEI)), in addition to an ID card number. By leveraging existing communication infrastructures, the mechanism would be able to guarantee the safety of electronic authentication, and to confirm that it demonstrates excellence in non-repudiation, authenticate user and mobile device which are used in the process of authentication, certification strength and also in comparison and analysis through experimenting with existing OTP mechanisms.

Keyword- Security, non-repudiation, multi factor authentication, IMEI,

1. INTRODUCTION

A credential is a piece of knowledge that enables individual access to computer based information systems[1]. User names and passwords are commonly used by people during a log in process to prove identity[2]. Passwords remain the most common mechanism for user authentication in computer security systems. This has various drawbacks, such as bad choices by users and vulnerability to capture [3],[4],[5]. An additional major problem is the fact that users tend to reuse passwords for different sites [6]. Some studies indicate that more than 70% of phishing activities are designed to steal user names and passwords. According to the anti-phishing working group (APWG)'s report [7], the number of malicious web pages designed to steal users' credentials at the end of Q2 in 2008 had increased by 258% over the same period in 2007. Therefore, protecting users' credentials from fraud attacks is extremely important. Many studies have proposed schemes to protect users' credentials against theft [8],[9],[10].

When a website only uses a user name and password as an authentication method, this method is known as one factor authentication (OFA). Another method is multi factor authentication (MFA). MFA means the use of more than one authentication factor in the authentication process [11],[12],[13].

Mobile authentication is one of the main methods of multi factor authentication. It uses mobile devices

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

(after install software token on mobile) for multi-factor authentication in place of other authentication methods such as hard tokens, smart tokens or smart chip cards. This requires the installation of software on a mobile device to generate a One Time Password (OTP)[14],[15],[16]. An OTP is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional authentication (such as usernames and passwords) [17].

Using a mobile device for authentication can be a challenge for the user. Many solutions currently being used by mobile applications either compromise security or usability [18]. There are some common drawbacks of using mobile devices to authenticate users:

- The user needs to enter a password periodically to start mobile applications [19]. Complex passwords are difficult to enter on mobile devices, and require frequent password entry. As a result of this the user will be compelled either to save the passwords on their devices or choose a weak password that they can easily enter onto their devices

- When the user's device is lost or stolen, a criminal can potentially get access to everything stored on the device. This is generally true nowadays for mobile phones and especially smart phones, which now outsell personal computers (PCs). Criminals have exploited this feature by stealing mobile devices and trying to sell them or access the user's personal information [20], If a user's device is stolen, the attacker can access the user's mobile and use it to generate OTPs. Meanwhile the attacker can perform both software attacks and physical attacks against the device.

An International Mobile Equipment Identity (IMEI) is a unique number to identify 3rd Generation Partnership Projects (3GPP). The IMEI number is used by a Global System for Mobile Communications (GSM) network to identify valid devices and therefore can be used for preventing access to a network from a stolen phone [21],[22].

In general, methods of certification are considered an essential requirement to authenticate a user when he/she requested service from the service provider, are divided into four, as in Table 1, depending on the element that becomes the basis of certification [23],[24],[25].

Classification	Description	Example
Type I	Something you know	Password, PIN
Type II	Something you have	Mobile Phone, Token, ID card number
Type III	Something you are	Iris, Fingerprint
Type IV	Something you do	Voice

TABLE 1. CLASSIFICATION OF AUTHENTICATION TYPE

An OTP mechanism creates a password only once along with additional features such as user certification and electronic transaction security to protect the user's information against leakage and at the same time solve the problem of having a static password mechanism. However, for electronic authentication it is not possible to establish face to face communication. In order to confirm the identity of a person accessing the system, the existing OTP mechanism faces problems such as not being able to guarantee certification (the identity of authenticity) and non repudiation [26],[27],[28].

This paper proposes a mechanism to improve the problems of existing OTP authentication and to guarantee certification and non-repudiation of users. The proposed system requires that each user register his or her personal information such as their ID card number, mobile number, IMEI, and PIN into the system. The server should offer this practical service. Server generate a one-time-password by combining the user's various forms of personal information (as above) and transmitting the created OTP to the user by encoding it after executing an Advanced Encryption Standard (AES) for it. The user registers his or her personal information at the registration phase. During the registration phase the server will verify IMEI validity, with reference to whether there is a valid IMEI number. The user will then transfer to the login phase for authentication by username and password.

When the user inserts a correct username and password, the server will transfer the user to a second authentication phase (a new layer) which is known as the confirmation phase. During this phase, the user will be compelled to insert his original personal information that had previously been provided for the system. This

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

layer combines two factors; something the user knows and something user has, after the user confirms these two factors and submits them to the server. The server will then generate an OTP and send it to the user by encrypted SMS. At this phase the server will verification the IMEI's validity while simultaneously providing certification guarantee and non repudiation because the OTP will not be sent directly to the user, while the server will check if the mobile device is in the same user's hand or not.

This paper is organized in the following order. Chapter 2, which follows the Introduction in Chapter 1 describes the existing research into OTPs, and Chapter 3 discusses secure authentication methods proposed in this research, Chapter 4 describes the experimental environment and the results of comparisons with existing mechanisms. Last but not least, Chapter V describes the conclusion of this research and some possible future research directions.

II. RELEVANT STUDIES

OTP authentication mechanisms are applied by utilizing various tools such as a hardware device (token device), or a software token (mobile phone) [29].

A. Hardware device (token device)

A token device is used to prove the user's identity in electronic authentication. This is done in some commercial transactions or in e-government services like that of New Zealand [30]. It is used in addition to or instead of a static login-ID to prove that the user is who they claim to be. The token acts like an electronic key in order to confirm the identity of a user when he/she is accessing the system[31].

Tokens contain some secret information that can be used to prove identity such as a static password token, a synchronous dynamic password token (The token and the authentication server must have synchronized clocks), and an asynchronous password token (by generating an OTP) [32],[33] ,[1].

A hardware token is considered more secure to use than user ID or passwords. It enhances the image of the organization by securing user credentials more effectively. However, the hardware may cause certain problems such as users always needing to carry the token with them and requiring multiple tokens for multiple websites. This does not provide full protection from man-in-the-middle attacks, and the hardware involves additional costs, such as the cost of the token and any replacement fees [14],[33],[34].

B. Software token (mobile phone)

A software token is a form of multi-factor authentication. Software tokens are stored on hardware devices such as mobile phones. Therefore, they are vulnerable to threats such as viruses and software attacks [33]. However, mobile phones are easily lost or stolen, if the mobile phone is in the wrong hands, a criminal can easily use personal data and most of the information is available without a great effort through services such as SMS [35].

Researchers try to solve the problems of security of authentication either by utilizing mobile phones as software tokens to generate an OTP which is then sent to the server[15],[36], or by using mobile phones as tools to receive an OTP from servers through SMS. In this case the system requires that the users log in to the system with a username and password and by correctly inserting credentials. Then the OTP code will be sent by mobile phone via SMS [37]. In both cases (the mobile phone as soft token and using a mobile phone just for receiving SMS) the authentication systems suffer from not guaranteeing the user's certification and non-repudiation [26],[27].

III. PROPOSED SYSTEM

By leveraging existing communication infrastructures, no additional costs are required for the proposed system. In any system of processing of electronic authentication, the identity, authenticity and non-repudiation of transactions are particularly important [38]. This paper resolved the problem of non repudiation during the authentication process and will contribute to the increased security of multi factor authentication process by sending the OTP only to trusted users.

A. Registration Phase

In the registration phase users are compelled to use their personal information (username, password, a 4-6

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

digit PIN, email, ID card number, and mobile number) in addition to International Mobile Equipment Identity (IMEI). Some algorithms will check IMEI for the user's mobile phone. If the IMEI not real, the user will be prevented from becoming registered in the system (system not safe wrong data). Thus the user is compelled to insert a real IMEI in the registration phase. Also, if IMEI and the mobile number are repeated (when registered by another user) the user will not able to complete his or her registration. The use of this method will ensure that every user has one mobile number and one IMEI number in addition to their ID card number. Mostly, authentication systems which are users of OTP authentication allow users to possess many accounts with the same mobile number. This will not happen in the proposed system, which will work to control the management of users' accounts and to reduce the errors in the users' information in the database. After the user is successfully registered, they will transfer to the login phase.

B. Traditional Login Phase

In this stage user will login into the system by using his username and password, if user insert wrong credentials (username and password) he will not able to accessing as in traditional login phase and he will still in this phase till insert correct one. After the user inserts a correct username and password as he or she enters the registration phase, the system will transfer the second user authentication phase (New layer of authentication).

C. *New Layer (Confirmation Phase)*

The creation of this layer will prevent the generation of the OTP by the server and prevent it being sent to user until the user confirms his or her personal information (PIN, mobile number, IMEI) which was registered in the previous phase (registration phase). Also, this layer will ensure the identity of authenticity and realize non-repudiation. In other authentication systems, after users submitted their credentials (username and password) to the system they can receive OTPs directly from the server by SMS. The proposed system will not generate OTPs and will not send anything to the user until the system ensures that the mobile device is in the right hand (in the hand of same user who request authentication). In this way the system will ensure the liability of the person that misuses the system. This layer combines two factors; something the user knows (PIN) and something user has (mobile number and IMEI). Applying this in one layer to confirm the identity of the user is considered a new idea.

Also, at this point the user can choose a method of receiving the OTP. If the user prefers not to receive the OTP by SMS he or she can receive it by email. Thus, in this layer the user will choose the method of receiving the OTP depending on what he prefers. If the user prefers to receive OTP by email, he demands to enter his email, PIN, and ID card number. In both cases (when the user prefers to receive OTP by SMS or by email) the user will receive an encrypted OTP by using Rijndael AES 256 and the decryption of the OTP will be conducted by PIN, which is a symmetric key between the user and the server. In case the user inserts the wrong information in confirmation phase server will redirect the user to the first login (traditional login) and the process of authentication will begin again.

If an adversary try to impersonate legal user shall get all user's information such as username and password (to pass from first login), steal user's mobile phone (to pass from confirmation phase and receive SMS), user's ID card number, user's email (username and password to access email), and PIN which is required in confirmation phase and for decrypt SMS or email.

D. Generating & Sending OTP

After the user passes through the confirmation phase, which will deal with the user reliably, the server will generate an OTP from the user's information. This may happen in two ways. The user may prefer to receive the OTP by mobile phone or may prefer to receive OTP by e-mail. This means that if users prefer to use mobile phones to receive OTPs, the elements which are demanded from user at the confirmation phase will contribute to the generation of OTP and the elements which are required from the user in the confirmation phase when he or she intends to receive OTP by email will contribute to the generation of OTP. In this way the future OTP cannot be predicated because the OTP will be totally different from one user to another. Also the OTP will be taken randomly from the user's info, so that the user will not get the same OTP when he or she uses the proposed system. In this paper the processes of Multi Factor Mechanism for

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Secure Authentication System are shown in the Figure1.

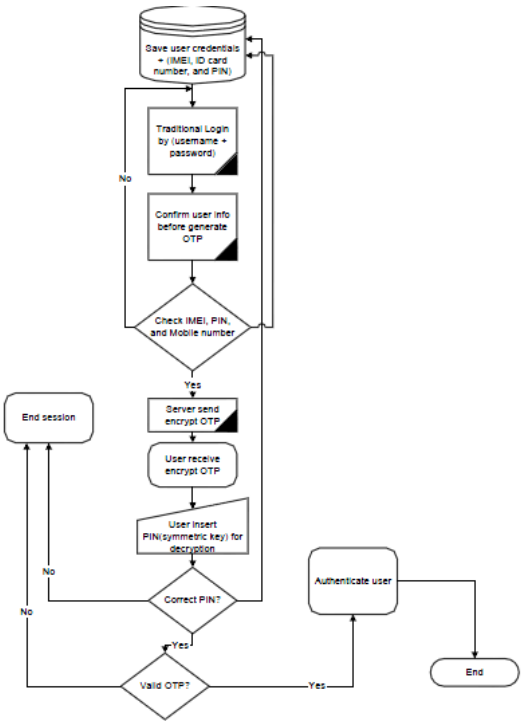


Fig. 1. Procedure of Proposed System

The server will send the encrypted OTP in the manner favoured by the user (SMS or email). After the user receives an encrypted message by OTP, he or she will transfer to another screen to prove the validity of his PIN and at the same time to decrypt the OTP (a symmetric key for encryption and decryption). If the PIN is wrong the session will end.

IV. COMPARISION ANALYSIS

A. Comparison and Analysis

In order to conduct a performance analysis of the proposed mechanism and the existing mechanism, comparison and analysis were executed on totally 8 performance evaluation elements such as non repudiation, long term password, tracking user, the block user's mobile phone, authenticated user and mobile phone, users' information reuse prevention, cell phone reuse prevention, and certification type**.**

Non-repudiation: Because the proposed mechanism works to authenticate the user and his or her mobile phone (IMEI plus mobile number), so the proposed system has all important information about the user such as ID card number, mobile number, and IMEI, all of which are unique. Thus the proposed system can ensure the liability of the person that misuses the system.

Long term password: A long password for authentication is generally considered to be more safe than a short one. However, humans have difficulty remembering complex or meaningless passwords [39]. At the confirmation phase, the user needs only to rewrite long term passwords such as (IMEI, the mobile number, or the ID card number) which they are already possess, or he/she can take it from his/her ID card or mobile phone, while the other system needs the user to remember these details.

Tracking user: Most authentication systems which generate OTP through the server and send the OTP to user by SMS cannot track whether the user is tampering with system because the authentication system only has the user's mobile number, in addition to their username and password. Thus a criminal could tamper with the system by receiving OTP through SMS and could then change or throw away the SIM card. While the proposed system can determine the liability of the person that misuses or tampering with system by using user's ID card number (unique number), in addition of mobile number (every user has unique mobile number and unique IMEI).

Block user's mobile: An International Mobile Equipment Identity (IMEI) is a unique number used by a Global System for Mobile Communications (GSM) network to identify valid devices. An IMEI can determine the position of a mobile device and also can blacklisting the device so that it becomes unusable on any network. The proposed system requires inserts in the IMEI to authenticate the user's device and to taking the necessary precautions in the event of tampering with the system. If the administrator of the proposed system discovers any attempts to tamper with the system he will be able to cancel the user's account and block the user and his or her mobile device from registering in the system. While an existing OTP system cannot prevent the use of the same device, the illegal user can return to register himself (if the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

administrator discovers illegal attempts being carried out by the user) as a legal user to access the system.

Authenticating users & mobile phones: Compared with other authentication systems which utilize mobile phone to generate OTPs or for receive SMS, these systems attempt to authenticate the user and neglect other parties which are used in the process of electronic authentication such as the user's mobile phone. However, the user is not the only party that needs to be authenticated to ensure the security of transactions on the Internet [40]. The proposed system works to authenticate both the user and mobile device, in addition to mutual authentication between the user and the server through a Secure Socket Layer (SSL).

User's information Reuse Prevention: The proposed system achieves a one-time password approach. Every user has totally unique information, which means there should be no need to separate the data as in other systems. This enhances privacy protection and minimises the probability of data matching.

Cellphone Reuse Prevention: The proposed system can prevent the cell phone from reuse by a criminal because the proposed system requires that every user has a unique phone number and a unique mobile device (IMEI), while indicating that the user's cell phone be lost or stolen. The attacker cannot use this by accessing system till gets other elements such as user's PIN or user's ID card number for the pass confirmation phase.

Certification type: Existing methods which utilize the user's mobile phone to receive SMS or to generate OTPs rely on what the user knows, while the proposed system depends on a combination of two factors - what the user knows and what the user owns (IMEI), In addition this method uses a new way to authenticate the use of a cell phone. It also works enhances security and operates as multi factor authentication inside multi factor authentication (nested multi factor authentication).

V. CONCLUSION

This paper proposed a mechanism of action for OTP authentication which can reinforce the security of authentication and the mechanism of guaranteeing non-repudiation by authenticating the user and the device which is used to receive encrypt OTPs. This cannot completely ensure the proper use of the system, but it can ensure the liability of the user that misuses the system. This mechanism requires the users presenting more information to prove proof their identity (in order to prove to the system that this user is the same user with the same device which is already registered in the system) unlike existing methods (such as utilizing the user's mobile phone to receive OTPs). Therefore the proposed method is suitable for areas in which security is crucial, such as providing authentication for internet banking, authentication for electronic payment, electronic governments authentication, and cloud computing authentication.

REFERENCES

[1] Shon Harris, *Access Control*, in *Mike Meyers' CISSP(R) Certification Passport*, Information Security Magazine, Editor 2002, McGraw-Hill Osborne Media. p. 422.

[2] Bander AlFayyadh, et al., *Improving Usability of Password Management with Standardized Password Policies*, 2011, Queensland University of Technology,: Australia,. p. 8.

[3] John Brainard, et al., *Fourth-factor authentication: somebody you know*. ACM, 2006: p. 1-11.

[4] Abdulaziz S. Almazyad and Y. Ahmad, *A New Approach in T-FA Authentication with OTP Using Mobile Phone.* Springer 2009. **58**: p. 9-17.

[5] Jiří Sobotka and Radek Doležel, *Multifactor authentication systems.* elektro revue, December 2010. **1**(1213-1539): p. 1-7.

[6] R.R.Karthiga and K.Aravindhan, *Enhancing Performance of User Authentication Protocol with Resist to Password Reuse Attacks.* International Journal Of Computational Engineering Research (IJCER), 2012. **2**(8): p. 106-115.

[7] Chun-Ying Huang, Shang-Pin Ma, and Kuan-TaChen, *Using one-time passwords to prevent password phishing attacks.* Science Direct, 2011.

[8] Chuan Yue and HAINING WANG, *BogusBiter: A Transparent Protection Against Phishing Attacks.* ACM, 2010. **10**(2): p. 31.

[9] Scott Garriss, et al., *Trustworthy and Personalized Computing on Public Kiosks*, in *6th international conference on Mobile systems, applications, and services*, 2008, ACM: USA. p. 199-210.

[10] Heng Yin, et al., *Panorama: capturing system-wide information flow for malware detection and analysis*, in *ACM conference on Computer and communications security*2007, ACM: USA. p. 116-127.

[11] Jing-Chiou Liou and Sujith Bhashyam, *A feasible and cost effective two-factor authentication for online transactions*, 2010, IEEEXplore: Chengdu, China p. 47-51.

[12] Jae-Jung Kim and Seng-Phil Hong, *A Method of Risk Assessment for Multi-Factor Authentication.* Journal of Information Processing Systems, 2011. **7**: p. 187-198.

[13] Do van Thanh, et al., *Strong authentication with mobile phone as security token.* IEEEXplore, 2009: p. 777-782.

[14] Trupti Hemant Gurav and Manisha Dhage, *Remote Client Authentication using Mobile phone generated OTP*. International Journal of Scientific and Research Publications, 2012. **2**(5): p. 4.

[15] Havard Raddum, Lars Hopland Nestas, and K.J. Hole', *Security Analysis of Mobile Phones Used as OTP Generators*, in *international conference on Information*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Security and Privacy of Pervasive Systems and Smart Devices, , International Federation for Information Processing (IFIP), Editor 2010, ACM: Berlin. p. 324-331.

[16] Gianluigi Me, Daniele Pirro, and R. Sarrecchia, *A mobile based approach to strong authentication on Web*, in *International Multi-Conference on Computing in the Global Information Technology*2006, IEEE Xplore. p. 67

[17] K.Aravindhan and R.R.Karthiga, *One Time Password: A Survey*. International Journal of Emerging Trends in Engineering and Development, 2013. **1**(3): p. 613-623.

[18] Hung-Min Sun, Yao-Hsin Chen, and Y.-H. Lin, *oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks.* IEEEXplore, 2012. **7**(2): p. 651- 663.

[19] Xing Fang and Justin Zhan, *Online Banking Authentication Using Mobile Phones*, in *5th International Conference on Future Information Technology (FutureTech)*,2010, IEEEXplore: Busan p. 1 - 5

[20] Mahendra Singh Bora and Amarjeet Singh, *Cyber Threats and Security for Wireless Devices.* Journal of Environmental Science, Computer Science and Engineering & Technology (JECET), 2013. **2**: p. 277-284.

[21] Jörg Eberspächer, et al., *GSM Architecture, Protocols and Services* 2009, John Wiley & Sons: UK. p. 327.

[22] GSM Association, *IMEI Allocation and Approval Guidelines*, Official Document TS.06 (DG06), Editor 2011. p. 33.

[23] Jae-Jung Kim and Seng-Phil Hong, *A Method of Risk Assessment for Multi-Factor Authentication.* Journal of Information Processing Systems,, 2011. **7**: p. 187--198.

[24] Kumar Abhishek, et al., *A Comprehensive Study on Multifactor Authentication Schemes.* 2013. **177**: p. 561-568.

[25] Jing-Chiou Liou and S. Bhashyam, *On Improving Feasibility and Security Measures of Online Authentication.* International Journal of Advancements in Computing Technology, October 2010. **2**(4.1): p. 11.

[26] Hyun-chul Kim, et al., *Design and Implementation of Multi Authentication Mechanism for Secure Electronic Commerce*, 2009, IEEEXplore: Seoul, South Korea, . p. 215-219.

[27] Milovanovic, M., et al., *Choosing Authentication Techniques in e-Procurement System in Serbia*, in *International Conference on Availability, Reliability and Security*2010, IEEE Xplore. p. 374- 379.

[28] Chii-Ren Tsai, *Non-Repudiation In Practice*, 2002, Second International Workshop for Asian Public Key Infrastructure (IWAP'02),: Taipei,Taiwan. p. 5.

[29] Jing-Chiou Liou and Sujith Bhashyam, *A feasible and cost effective two-factor authentication for online transactions*, in *2nd International Conference of Software Engineering and Data Mining (SEDM)*2010, IEEEXplore: Chengdu, China p. 47 - 51

[30] Yu-Cheng Tu and C. Thomborson, *Preliminary Security Specification for New Zealand's igovt System.* Australian Computer Society, Inc, 2009. **98**: p. 10.

[31] Nermin Hamza and Dr.Bahaa El-Din M.Hassan, *A Dynamic ID-based authentication scheme with smart token*, in *Computer Engineering & Systems, 2009. ICCES 2009.*2009, IEEEXplore: Cairo p. 294 - 299

[32] H. Karen Lu and Asad Ali, *Communication Security between a Computer and a Hardware Token* in *Third International Conference on Systems, ICONS* 2008, IEEEXplore: Cancun p. 220 - 225

[33] Manav Singhal and Shashikala Tapaswi, *Software Tokens Based Two Factor Authentication Scheme.* International Journal of Information and Electronics Engineering, 2012. **2**: p. 383-386.

[34] Gauri Rao and Dr. S.H. Patil, *THREE DIMENSIONAL VIRTUAL ENVIRONMENT FOR SECURED AND RELIABLE AUTHENTICATION.* Journal of Engineering Research and Studies (JERS), 2011. **2**(2): p. 68-73.

[35] David Lisoněk and Martin Drahanský, *SMS Encryption for Mobile Communication.* IEEEXplore, 2008: p. 198-201.

[36] Fadi Aloul, Syed Zahidi, and Wassim El-Hajj, *Two Factor Authentication Using Mobile Phones.* IEEEXplore, 2009: p. 641-644.

[37] D.Parameswari and L.Jose, *SET with SMS OTP using Two Factor Authentication.* Journal of Computer Applications (JCA), 2011. **4**(4): p. 4.

[38] Xian-ge Huang, Lei Shen, and Yan-hong Feng, *A User Authentication Scheme Based on Fingerprint and USIM Card*, in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP)*,2008, IEEEXplore: Harbin p. 1261 - 1264.

[39] Sonia Chiasson, et al. *Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords*. in *16th ACM conference on Computer and communications security (CCS)*. 2009. New York: ACM.

[40] Audun Jøsang, et al., *Service Provider Authentication Assurance*, in *Tenth Annual International Conference on Privacy, Security and Trust*2012, IEEE Xplore. p. 203-210.

IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2013
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

ISSN 1947 5500
http://sites.google.com/site/ijcsis/